PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-287192

(43)Date of publication of application : 13.10.2000

(51)Int.Cl. H04N 7/167
G09C 1/00
H04L 9/08
H04L 9/32
H04L 12/56

(21)Application number : 11-093916

(22)Date of filing : 31.03.1999

(71)Applicant : TOSHIBA CORP

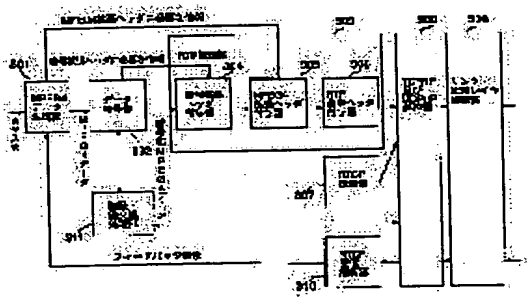
(72)Inventor : SAITO TAKESHI
KATO HIROSHI
TOMOTA ICHIRO
TAKAHATA YOSHIAKI
AMI JUNKO

(54) INFORMATION DISTRIBUTING DEVICE, RECEIVING DEVICE AND COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To extend copy protection technique to a digital contents circulation by executing a transport protocol processing required for transferring contents information, creating a basic transport header which indicates that contents information is enciphered and transmitting a packet including desired information to a communication opposite party by way of a network.

SOLUTION: MPEG4 data outputted from an MPEG4 data creating part 301 are enciphered by a data enciphering part 302. An authentication and key exchange processing part 311 generates a new cipher key for an enciphering processing in the case of the updating timing of the cipher key and gives it to the data enciphering part 302. Together with it, the value of information to be a source for generating a common key is increased and given to the part 302. The value of information to be the source for generating the common key is given from the part 302 to a cipher extension header giving part 304. An MPEG4 extending header is exempted from a ciphering object.



LEGAL STATUS

[Date of request for examination] 19.03.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－287192
（P2000－287192A）
(43)公開日　平成12年10月13日(2000.10.13)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04N	7/167		H04N	7/167	Z　5C064
G09C	1/00	640	G09C	1/00	640Z　5J104
H04L	9/08		H04L	9/00	601C　5K030
	9/32				675A　9A001
	12/56			11/20	102F

審査請求　未請求　請求項の数15　ＯＬ　（全 25 頁）

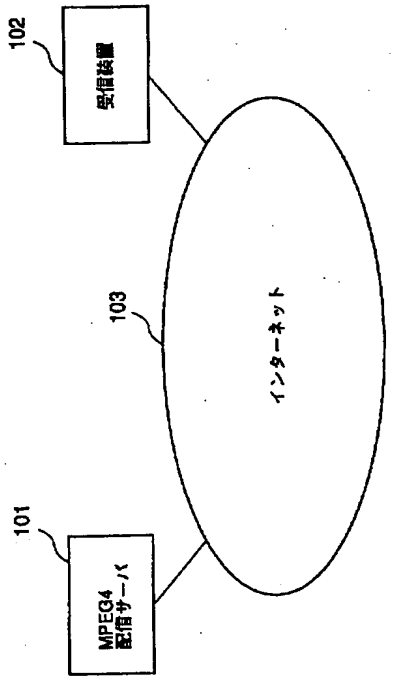
(21)出願番号　特願平11－93916
(22)出願日　平成11年３月31日(1999.3.31)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　加藤　拓
東京都府中市東芝町１番地　株式会社東芝府中工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　情報配信装置、受信装置及び通信方法

(57)【要約】
【課題】　コピープロテクション技術をＩＥＥＥ１３９４のみならずインターネット上のコンテンツ流通にも拡張可能な情報配信装置を提供すること。
【解決手段】　コンテンツを暗号化してインターネット経由で受信装置に配信する配信装置であって、受信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行ない、所定の符号化方式で符号化されたコンテンツを暗号化し、転送されるコンテンツが暗号化されたものであるか否かを示す属性情報および該コンテンツの暗号方式を示す属性情報のうちの少なくとも一方の属性情報を含む暗号化に関する属性情報からなる暗号拡張ヘッダを作成し、コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成し、基本トランスポートヘッダと暗号拡張ヘッダと暗号化されたコンテンツ情報とを含むパケットを送出する。



1

【特許請求の範囲】

【請求項１】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、

前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、

所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、

前記暗号化に関する属性情報および前記符号化方式を示す情報を含む暗号拡張ヘッダを作成する手段と、

前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたものである旨を示す情報を含む基本トランスポートヘッダを作成する手段と、

前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする情報配信装置。

【請求項２】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、

前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、

所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、

前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、

前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたものである旨および該コンテンツ情報の符号化方式を示す情報を含む基本トランスポートヘッダを作成する手段と、

前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする情報配信装置。

【請求項３】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、

前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、

所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、

前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、

前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、

前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備え、

前記基本トランスポートヘッダには、少なくとも転送されるコンテンツ情報が暗号化された可能性を有するものである旨を示す情報を記述し、

前記暗号拡張ヘッダには、少なくとも転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報を記述し、

前記基本トランスポートヘッダまたは前記暗号拡張ヘッダには、前記コンテンツ情報の符号化方式を示す情報をも記述することを特徴とする情報配信装置。

【請求項４】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、

前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、

所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、

前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、

前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、

前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備え、

前記暗号拡張ヘッダには、転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報および転送されるコンテンツ情報の暗号方式を示す情報のうちの少なくとも一方を記述することを特徴とする情報配信装置。

【請求項５】前記暗号拡張ヘッダを前記パケットのパケットヘッダ内の拡張ヘッダとすることを特徴とする請求項１ないし４のいずれか１項に記載の情報配信装置。

【請求項６】前記暗号拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとすることを特徴とする請求項１ないし４のいずれか１項に記載の情報配信装置。

【請求項７】前記コンテンツ情報の属性情報を含むコンテンツ拡張ヘッダを作成する手段を更に備え、

前記コンテンツ拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとすることを特徴とする請求項１ないし６のいずれか１項に記載の情報配信装置。

【請求項８】前記コンテンツ拡張ヘッダは暗号化しないことを特徴とする請求項７に記載の情報配信装置。

【請求項９】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、

前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、

前記認証処理の後に前記情報配信装置から、基本トラン

スポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、
前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、前記暗号拡張ヘッダに含まれる前記暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする情報受信装置。

【請求項１０】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、
前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、
前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、
前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化された可能性を有するものであることが示されている場合、前記暗号拡張ヘッダを参照して暗号化の有無を調べ、暗号化されたものであるならば、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする情報受信装置。

【請求項１１】前記基本トランスポートヘッダまたは前記暗号拡張ヘッダを参照して前記コンテンツ情報の符号化方式を調べる手段を更に備えたことを特徴とする請求項９または１０に記載の情報受信装置。

【請求項１２】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、
前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、
前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、
前記暗号拡張ヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする情報受信装置。

【請求項１３】受信した前記基本トランスポートヘッダを参照して一定以上の遅延時間または一定以上のパケット廃棄が確認された場合に、前記情報配信装置に対して所定の暗号化パラメータの送信を要求する手段を更に備えたことを特徴とする請求項９ないし１２のいずれか１項に記載の情報受信装置。

【請求項１４】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置の通信方法であって、
前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行ない、

所定の符号化方式で符号化されたコンテンツ情報を暗号化し、
転送されるコンテンツ情報が暗号化されたものであるか否かを示す属性情報および該コンテンツ情報の暗号方式を示す属性情報のうちの少なくとも一方の属性情報を含む前記暗号化に関する属性情報からなる暗号拡張ヘッダを作成し、
前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成し、
前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出することを特徴とする通信方法。

【請求項１５】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置の通信方法であって、
前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行ない、
前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信し、
前記暗号拡張ヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号することを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット等のネットワークを介したデータ送受信を著作権保護を考慮して行う情報配信装置、受信装置及び通信方法に関する。

【０００２】

【従来の技術】近年、デジタル放送の開始や、デジタルＡＶ機器の発売等、いわゆる「家庭ＡＶ環境のデジタル化」が大きな注目を集めている。デジタルＡＶデータは、様々な圧縮が可能、マルチメディアデータとしての処理が可能、何回再生しても劣化が無い、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【０００３】しかしながらその反面、このデジタルＡＶ技術には、「コンテンツの不正コピーを容易に行うことができる」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元通りの品質でしかも恒久的に劣化の無い複製が作成されてしまうため、いわゆる「不正コピー」の問題が発生する。

【０００４】そこで、この「不正コピー」を防ぐための技術が種々検討されている。その中の一つが、ＣＰＴＷ

5

Ｇ（コピープロテクション技術ワーキンググループ）で検討されている「１３９４ＣＰコンテンツ保護システム仕様（１３９４ＣＰ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ ＳｙｓｔｅｍＳｐｅｃｉｆｉｃａｔｉｏｎ）」である。この技術は、ＩＥＥＥ１３９４バスに接続されたノード間で、転送するコンテンツ（例えばＭＰＥＧデータ等）について、送受信ノードの間で予め認証手続きをおこない、暗号鍵（コンテンツキー）を共有できるようにしておき、以降はそのコンテンツをその暗号鍵で暗号化して転送し、認証手続きを行った両ノード以外のノードにはそのコンテンツが復号化できないようにする技術である。このようにすることにより、認証を行っていないノードは、暗号鍵の値がわからないため、転送されているデータ（すなわち暗号化されたコンテンツデータ）をたとえ取り込むことができたとしても、このデータを復号化することはできない。このような認証に参加できるノードを、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、コンテンツの不正コピーを予め防ぐことが可能になる。

【０００５】

【発明が解決しようとする課題】さて、デジタルコンテンツの流通は、当然ながらＩＥＥＥ１３９４上に限定されるものではなく、ネットワーク一般に対して期待される。公衆網や、物理／リンクネットワークにとらわれない技術インフラとして、インターネットは、その有力な候補となろう。

【０００６】しかしながら、現在はインターネット上のデジタルコンテンツ（特にデジタルＡＶストリーム）の流通は、著作権保護のなされないまま、生のデータのままでＲＴＰ（リアルタイムトランスポートプロトコル）上を転送される方式が主流となっている。

【０００７】本発明は、上記事情を考慮してなされたもので、コピープロテクション技術をＩＥＥＥ１３９４のみならずインターネット等のネットワーク上のデジタルコンテンツ流通にも拡張することの可能な情報配信装置、受信装置及び通信方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明（請求項１）は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報および前記符号化方式を示す情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたものである旨を示す情報を含む基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする。

6

【０００９】本発明（請求項２）は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたものである旨および該コンテンツ情報の符号化方式を示す情報を含む基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする。

【００１０】本発明（請求項３）は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備え、前記基本トランスポートヘッダには、少なくとも転送されるコンテンツ情報が暗号化された可能性を有するものである旨を示す情報を記述し、前記暗号拡張ヘッダには、少なくとも転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報を記述し、前記基本トランスポートヘッダまたは前記暗号拡張ヘッダには、前記コンテンツ情報の符号化方式を示す情報をも記述することを特徴とする。

【００１１】本発明（請求項４）は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ

情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備え、前記暗号拡張ヘッダには、転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報および転送されるコンテンツ情報の暗号方式を示す情報のうちの少なくとも一方を記述することを特徴とする。

【００１２】好ましくは、前記暗号拡張ヘッダには、転送されるコンテンツ情報の符号化方式を示す情報をも記述するようにしてもよい。

【００１３】好ましくは、前記暗号拡張ヘッダを前記パケットのパケットヘッダ内の拡張ヘッダとするようにしてもよい。

【００１４】好ましくは、前記暗号拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとするようにしてもよい。

【００１５】好ましくは、前記コンテンツ情報の属性情報を含むコンテンツ拡張ヘッダを作成する手段を更に備え、前記コンテンツ拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとするようにしてもよい。

【００１６】好ましくは、前記コンテンツ拡張ヘッダは暗号化しないようにしてもよい。

【００１７】本発明（請求項９）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、前記暗号拡張ヘッダに含まれる前記暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする。

【００１８】本発明（請求項１０）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化された可能性を有するものであることが示されている場合、前記暗号拡張ヘッダを参照して暗号化の有無を調べ、暗号化されたものであるならば、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする。

【００１９】好ましくは、前記基本トランスポートヘッダまたは前記暗号拡張ヘッダを参照して前記コンテンツ情報の符号化方式を調べる手段を更に備えるようにしてもよい。

【００２０】本発明（請求項１２）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記暗号拡張ヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする。

【００２１】好ましくは、受信した前記基本トランスポートヘッダを参照して一定以上の遅延時間または一定以上のパケット廃棄が確認された場合に、前記情報配信装置に対して所定の暗号化パラメータの送信を要求する手段を更に備えるようにしてもよい。

【００２２】本発明（請求項１４）は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置の通信方法であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行ない、所定の符号化方式で符号化されたコンテンツ情報を暗号化し、転送されるコンテンツ情報が暗号化されたものであるか否かを示す属性情報および該コンテンツ情報の暗号方式を示す属性情報のうちの少なくとも一方の属性情報を含む前記暗号化に関する属性情報からなる暗号拡張ヘッダを作成し、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成し、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出することを特徴とする。

【００２３】本発明（請求項１５）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置の通信方法であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続の少なくとも一方を含む認証処理を行ない、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信し、前記暗号拡張ヘッダ

により前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号することを特徴とする。

【００２４】本発明によれば、送信側において、ＲＴＰ（リアルタイムトランスポートプロトコル）やＨＴＴＰ（ハイパーテキストトランスファープロトコル）トランスポートプロトコルにおける拡張ヘッダあるいはペイロードヘッダの形で、暗号拡張ヘッダを設け、該暗号拡張ヘッダに暗号化に関する属性情報（例えば、暗号化の有無、暗号方式、コピー属性に関する情報（暗号モードインジゲータ）、コンテンツキー（共通鍵）を生成するもととなる情報（Ｅｖｅｎ／Ｏｄｄフィールド）、等）を記述することにより、送信側から受信側に安全にコンテンツデータを転送し、また受信側においてペイロードにて転送される暗号化されたコンテンツデータを復号することができる。

【００２５】また、従来のＲＴＰでは、そのペイロードタイプフィールドに、「ペイロードに格納されているデータの符号化方式」が記載されているのみで、ペイロードに格納されているデータが、（ネットワークレイヤや、トランスポートレイヤではなくて）コンテンツレイヤにて暗号化されていた場合に、これを相手側装置に通知する方法がなかったが、本発明によれば、ＲＴＰのペイロードタイプフィールドに「暗号化データ」あるいは「暗号化された特定の符号化方式で符号化されたデータ」である旨を記述できるため、これを相手側装置に通知することができるようになり、もって、前述の暗号化されたコンテンツの送受が行えるようになる。

【００２６】このように本発明によれば、ＡＶストリーム伝送のコピープロテクション技術をＩＥＥＥ１３９４のみならずインターネット等のネットワーク上のデジタルコンテンツ流通にも拡張するが可能となる。

【００２７】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００２８】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００２９】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００３０】（第１の実施形態）図１に、本実施形態における情報配信システムの構成例を示す。図１では、インターネット１０３に本実施形態に係るＭＰＥＧ４配信サーバ１０１および受信装置１０２が接続されており、

インターネット１０３を通してＭＰＥＧ４配信サーバ１０１と受信装置１０２との間でＭＰＥＧ４のＡＶストリームの秘匿通信を行うものである。もちろん、インターネット１０３には他のＭＰＥＧ４配信サーバや受信装置あるいはその他の種類の機器が接続されていてもかまわない。

【００３１】また、本実施形態では、データの種別をＭＰＥＧ４として説明するが、もちろん他の種別のデータにも本発明は適用可能である。

【００３２】このＭＰＥＧ４配信サーバ１０１は、受信装置１０２に対して、ＭＰＥＧ４データの配信を行う。ＭＰＥＧ４データは、ファイル転送の形ではなく、ストリーム配信の形をとる。このとき、著作権保護の対象とするＭＰＥＧ４データは、暗号化した状態で配信する。その際、配信に先立って、ＭＰＥＧ４配信サーバ１０１と受信装置１０２との間で、認証手続きや認証鍵の交換の手続きなどを行う。

【００３３】このときのシーケンスの一例を図２に示す。

【００３４】なお、図２は、いわゆるコンテンツレイヤの暗号化や認証について示したものであり、ＩＰレイヤあるいはトランスポートレイヤ等のレイヤにおけるセキュリティやそれらレイヤでの認証手続き等に関しては省略してあり、またコンテンツレイヤで先立って行われる課金などの手続きも省略してある（課金処理や他レイヤのでの認証／暗号処理が行われない場合もあり得る）。

【００３５】ここでは、受信装置１０２がＭＰＥＧ４配信サーバ１０１に対して配信の要求を行う場合を考える。この場合は、最初の認証要求は受信装置１０２から送出される（Ｓ２０１）。認証要求では、その機器（受信装置１０２）が予め定められた認証機関から「著作権保護を受けたコンテンツのやりとりを行うことのできる機器である」との証明を受けている証書（ｃｅｒｔｉｆｉｃａｔｅ、機器証明）の交換も同時に行ってもよい。

【００３６】ここで、機器証明の際に用いる「機器のＩＤ」は、ＩＰアドレスを使用してもよいが、ＩＰアドレスはＤＨＣＰサーバなどで与えられる場合には、装置のブート毎に可変の値になってしまう可能性がある。そこで、機器証明で使われる機器ＩＤとしては、その装置のＭＡＣアドレス、あるいはＥＵＩ６４アドレス、あるいはそれらのアドレスに部品モジュール番号を付与したものなどを利用してもよい。また、その装置のＣＰＵの識別番号や、ＭＰＥＧ４デコーダの識別番号等、（理想的には）世界唯一であると考えられる数値（あるいは、その地域で唯一、等、同一な値がほとんど期待されない数値）を、「機器のＩＤ」として用いてもよい。

【００３７】受信装置１０２からのメッセージを受信したＭＰＥＧ４配信サーバ１０１は、認証要求の応答と、証書（機器証明）の交換を行う（Ｓ２０２）。

【００３８】次に、ＭＰＥＧ４配信サーバ１０１および

受信装置１０２は、共通の認証鍵を生成するために、認証鍵の生成プロセスを行う（Ｓ２０３）。この手続きの詳細については、例えばＩＥＥＥ１３９４のコピープロテクションの認証鍵の生成プロセスと同様のものであってもよい。このプロセスが終了すると、ＭＰＥＧ４配信サーバ１０１および受信装置１０２は共通の認証鍵Ｋａｕｔｈを、第３者に知られることなく、共有することができる。

【００３９】次に、ＭＰＥＧ４配信サーバ１０１は、交換鍵Ｋｘと認証鍵Ｋａｕｔｈとの排他的論理和（Ｋｘ EX-OR Ｋａｕｔｈ）と乱数Ｎｃを受信装置１０２に送信する（Ｓ２０４，Ｓ２０５）。受信装置１０２では、受信した（Ｋａｕｔｈ EX-OR Ｋｘ）の値と（Ｋａｕｔｈ）の値との排他的論理和を計算して（Ｋｘ EX-OR Ｋａｕｔｈ EX-OR Ｋａｕｔｈ＝Ｋｘ）、交換鍵Ｋｘを取り出す。

【００４０】この時点で、ＭＰＥＧ４配信サーバ１０１および受信装置１０２は、認証鍵Ｋａｕｔｈ、交換鍵Ｋｘ、乱数Ｎｃという３種類の数値を共有していることになる。

【００４１】ここで、暗号鍵（コンテンツキー）Ｋｃ、すなわちＭＰＥＧ４配信サーバ１０１が送信すべきＭＰＥＧ４データを暗号化するための暗号鍵であって且つ受信装置１０２が受信した暗号化されたＭＰＥＧ４データを復号化するための暗号鍵（共有鍵）Ｋｃは、ＭＰＥＧ４配信サーバ１０１および受信装置１０２の各々において、予め定められた同一の関数Ｊを用いることにより、上記の数値の一部の関数として算出される。例えば、Ｋｃ＝Ｊ［Ｋｘ，ｆ（ＥＭＩ），Ｎｃ］と算出される。ここで、ＥＭＩとは、「そのデータ（コンテンツ）のコピー属性」を意味し、「そのデータは無制限にコピー可能であるか、それとも１回だけコピー可能であるか、それとも２回だけコピー可能であるか、それとも無条件にコピー不可であるか、コピー済みでこれ以上コピー不可であるか、…」等の属性をあらわす。この属性値ＥＭＩをある特定の関数ｆで変換したものがｆ（ＥＭＩ）である。これらの関数Ｊやｆは、外部に対して秘密であっても良い。

【００４２】さて、暗号鍵Ｋｃが生成された後、ＭＰＥＧ４配信サーバ１０１は、この暗号鍵Ｋｃでコンテンツ（ＭＰＥＧ４データ）を暗号化して、インターネット上に転送する（Ｓ２０６，Ｓ２０７，…）。

【００４３】なお、後述するように、暗号化コンテンツは「ＡＶストリームデータのリアルタイム転送」の形を取りつつインターネット上を転送されるため、トランスポートプロトコルとしてはＲＴＰ（リアルタイムトランスポートプロトコル）が採用される。

【００４４】また、この暗号鍵Ｋｃは時変にする（すなわち、ある時間が経過すると値が変わる）。例えば、前回の変更時から所定の時間（所定の時間は、一定でもよいし、可変でもよい）が経過したことが認識された場合に、変数Ｎｃの値をインクリメントし、再度、上記の関数Ｊを用いて暗号鍵Ｋｃの値を計算する。このとき、暗号化Ｋｃの値を更新するタイミング（あるいはどのデータから使用する暗号鍵Ｋｃを更新するか）を送受信側で同期して認識する必要がある。このため、転送されるＭＰＥＧ４データ（ＡＶデータ）に、Ｅｖｅｎ／Ｏｄｄフィールドなる領域を設け、このフィールドの値の変わり目を、変数Ｎｃの値、ひいては暗号鍵Ｋｃの値の変わり目と規定する（当該データから更新後の暗号鍵Ｋｃが適用される）。

【００４５】すなわち、ＭＰＥＧ４配信サーバ１０１では上記時間の経過を監視し、暗号鍵Ｋｃを更新するタイミングになったことが検出された場合、変数Ｎｃの値をインクリメントして暗号鍵Ｋｃの値を計算し直し、この再計算後の暗号鍵Ｋｃを使用して送信すべきＭＰＥＧ４データを暗号化するとともに、Ｅｖｅｎ／Ｏｄｄフィールドの値をインクリメントさせて、送信を行う。以降は、次の更新タイミングまで、この暗号鍵Ｋｃを使用して暗号化を行う。一方、受信装置１０２では、受信したＥｖｅｎ／Ｏｄｄフィールドの値を監視し、その値が直前に受信した値に比較してインクリメントされていることが検出された場合、変数Ｎｃの値をインクリメントして暗号鍵Ｋｃの値を計算し直し、この再計算後の暗号鍵Ｋｃを使用して受信した暗号化データを復号化する。以降、次にＥｖｅｎ／Ｏｄｄフィールドの値の変化が検出されるまで、この暗号鍵Ｋｃを使用して復号化を行う。

【００４６】このようにして、ＭＰＥＧ４配信サーバ１０１と受信装置１０２間で暗号化されたＭＰＥＧ４データのやり取りがなされる。

【００４７】図３に、ＭＰＥＧ４配信サーバ１０１の内部構成例を示す。

【００４８】図３に示されるように、本実施形態のＭＰＥＧ４配信サーバ１０１は、ＭＰＥＧ４データ生成部３０１、データ暗号部３０２、暗号拡張ヘッダ付与部３０４とＭＰＥＧ４拡張ヘッダ付与部３０５とＲＴＰ基本ヘッダ付与部３０６を含み、ＲＴＰの処理を行うＲＴＰ処理部３０３、ＲＴＣＰ送信部３０７、ＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部３０８、リンク・物理レイヤ処理部３０９、ＲＴＣＰ受信解析部３１０、認証・鍵交換処理部３１１を備えている。

【００４９】図２のシーケンスの認証や暗号に関する処理（Ｓ２０１～Ｓ２０５までの処理）および暗号鍵更新に関する処理は、認証・鍵交換処理部３１１により行われる。

【００５０】さて、入力されたＡＶ入力（例えばアナログ信号）は、ＭＰＥＧ４データ生成部３０１にてＭＰＥＧ４のデータに圧縮される。

【００５１】このとき、「どこがＩピクチャか」、「符号化レートはいくらか」等、生成しているＭＰＥＧ４に

ついての属性情報をＭＰＥＧ４データ転送時に同時に受信側に通知すると、受信側においてその再生（復号）処理が行いやすくなる場合がある。特にインターネットでは、転送するパケットの廃棄、遅延、到着順の変更等が起こり得るため、それらの属性情報を得ることは、受信側で高品質に再生するためには欠かせない情報である。例えば、本実施形態のＭＰＥＧ４の場合であれば、ＶＯＰヘッダに関する情報等がこれにあたる。また、ＭＰＥＧ４システムに関わる情報、例えば、Ｓｙｎｃ　Ｌａｙｅｒによる同期情報の伝達や、複数ＭＰＥＧ４ストリームを多重化して送信する場合の多重化のための情報あるいはオブジェクトディスクリプタの初期値や最新値に関わる情報等が必要な場合も考えられる。このため、ＡＶデータをＲＴＰにて転送する場合には、ＲＴＰの拡張ヘッダまたはＲＴＰペイロードのペイロードヘッダという形で、送信するＡＶデータと並行して属性情報を送ることが行われる。

【００５２】本実施形態では、これらの属性情報がＲＴＰ拡張ヘッダの形で送信されるものとする。すなわち、「ＭＰＥＧ４拡張ヘッダ」なる種別（ＩＤ）のＲＴＰ拡張ヘッダとして送信される。このため、ＭＰＥＧ４データ生成部３０１からＭＰＥＧ４拡張ヘッダ付与部３０５に対して必要な情報が通知される。

【００５３】次に、ＭＰＥＧ４データ生成部３０１から出力されたＭＰＥＧ４データをデータ暗号部３０２が暗号化する。その際に使用する暗号鍵は、前述の時変の暗号鍵Ｋｃである。また、この暗号処理についても、種々の属性情報が考えられ、本実施形態では「暗号拡張ヘッダ」なる種別（ＩＤ）のＲＴＰ拡張ヘッダが暗号拡張ヘッダ付与部３０４にて付与される。このため、データ暗号部３０２から暗号拡張ヘッダ付与部３０４に対して必要な情報が通知される。

【００５４】なお、上記の暗号処理のために、認証・鍵交換処理部３１１では、暗号鍵Ｋｃの更新のタイミングになった場合には、Ｎｃをインクリメントして前述の関数Ｊにより新たな暗号鍵Ｋｃを生成してデータ暗号部３０２に渡す。また、これとともに、前述のＥｖｅｎ／Ｏｄｄフィールドの値をインクリメントして、データ暗号部３０２に渡す。Ｅｖｅｎ／Ｏｄｄフィールドの値は、上記のようにデータ暗号部３０２から暗号拡張ヘッダ付与部３０４に渡される。

【００５５】ここで、図４に、暗号拡張ヘッダの一例を示す。図４に示されるように、この暗号拡張ヘッダには、拡張ヘッダ種別フィールド、暗号化有無フィールド、暗号方式表示フィールド、暗号モードインジゲータ（ＥＭＩ）フィールド、Ｅｖｅｎ／Ｏｄｄフィールドがある。拡張ヘッダ種別フィールドは、当該拡張ヘッダの種別を示す情報を記述するためのフィールドである。この場合、拡張ヘッダ種別フィールドには暗号拡張ヘッダを示す情報が記述される。暗号化有無フィールドは、当

該ＲＴＰパケットで転送されるデータが暗号化されたものであるか否かを示す情報を記述するためのフィールドである。暗号方式表示フィールドは、当該ＲＴＰパケットで転送されるデータに対して使用する暗号方式を示す情報を記述するためのフィールドである。例えば、暗号方式がＭ６であることを示す情報が記述される。暗号モードインジゲータ（ＥＭＩ）フィールドは、前述のコピー属性値ＥＭＩを記述するためのフィールドである。Ｅｖｅｎ／Ｏｄｄフィールドは、前述した通り、送信側から受信側に対して暗号鍵の更新タイミングを通知するためのフィールドである。

【００５６】なお、ここでは、各フィールドは一例として８ビットとしているが、これに限定されるものではなく、適宜定めることが可能である。

【００５７】ここで、あるＡＶデータを暗号化して受信側に送ると、早送り等のトリックプレイを行ったりあるいは部分的な静止画像を送ったりしたいときなどに受信側での処理が困難になる場合がある。これは、暗号化されたＡＶストリームの内の一部分だけを送信するという作業に困難を伴うからである（例えば、Ｎｃの値がインクリメントではなく、いくつか飛んでしまう、等の理由による）。このため特定の場合に受信側に対してＡＶデータに暗号をかけずに送信したいという場合が考えられる。この場合、受信側に対して「このＡＶデータには暗号をかけています／いません」といった情報を通知する機構が必要となる。上記の暗号化有無フィールドは例えばこの目的で使われる。

【００５８】また、「あるストリームについてはこの暗号方式、別のあるストリームについてはこの暗号方式」といったように、インターネット上では、異なる暗号方式が共存する可能性がある。このような場合、「このＡＶデータは、どの暗号方式で暗号化されているか」を示すフィールドがあると、受信側では、このフィールドを見て、適当な復号化エンジンを選択して、暗号を復号化することができるようになる。上記の暗号方式表示フィールドは例えばこの目的で使われる。

【００５９】また、図４に示すように、暗号モードインジゲータ（ＥＭＩ）フィールドには、ＩＥＥＥ１３９４の場合の２ビットと異なり、８ビット用意してある。これは、「このＡＶデータはＮ回までコピー可能」という情報を通知する場合にそのＮの数値の選択に自由度を持たせることや、特殊なコピーを認める場合（例えば、ある条件が満たされているときに限りコピーを可能とする場合）などに、このフィールドの値が多くの値を取れるようにしておくことで、それらに対応できるようにするためである。

【００６０】また、図４に示すように、Ｅｖｅｎ／Ｏｄｄフィールドには、ＩＥＥＥ１３９４の場合と１ビットと異なり、８ビット用意してある。これは、前述のようにインターネットではパケットの廃棄、遅延、到着順の

逆転が起こり得ることから、１ビットの情報量では充分ではないとの配慮からである。すなわち、例えばインターネットではＳ２０７に示すようなＥｖｅｎ／Ｏｄｄビット＝１のパケットがすべて廃棄されるような場合が想定し得る。この場合、Ｅｖｅｎ／Ｏｄｄフィールドを１ビットとすると、次のパケットではＥｖｅｎ／Ｏｄｄビットは０に戻ってしまうため、受信側から見ると「Ｅｖｅｎ／Ｏｄｄビットが０である状態が継続されている（Ｅｖｅｎ／Ｏｄｄビットに変化はない）」と認識されてしまう。このように、実際にはＮｃは２つインクリメントされるべきであるのに、Ｅｖｅｎ／Ｏｄｄビットの値が変わっていないと認識されることで、Ｎｃの値のインクリメントがなされず、正しい暗号鍵の生成ができない、という問題点が発生し得る。そこで、Ｅｖｅｎ／Ｏｄｄフィールドには、２ビット以上、例えば８ビット用意し、インターネットにおけるパケット廃棄／遅延／到着順逆転が起こっても、受信側が適切な処理ができるように配慮してある。

【００６１】ここで、本実施形態においては、データの暗号化は、ＭＰＥＧ４データそのものに対してのみ行われ、ＭＰＥＧ４拡張ヘッダに対しては行われない。ＭＰＥＧ４拡張ヘッダは、いわゆる「著作権を守るべきコンテンツ」ではなく、受信側にてＭＰＥＧ４データそのものを使用するのに先立って使用されるものであるため、これは暗号化の対象から外している。

【００６２】結局、ＲＴＰ処理部３０３では、暗号拡張ヘッダ付与部３０４にて暗号拡張ヘッダが、ＭＰＥＧ４拡張ヘッダ付与部３０５にてＭＰＥＧ４拡張ヘッダが、ＲＴＰ基本ヘッダ付与部３０６にてＲＴＰ基本ヘッダが、それぞれ付与され、図５に示すような形のＲＴＰヘッダが付与されることになる。ここで、暗号拡張ヘッダはデータ暗号部３０２からの情報に基づいて生成され、ＭＰＥＧ４拡張ヘッダはＭＰＥＧ４データ生成部３０１からの情報に基いて生成される。また、ＲＴＰヘッダは、タイムスタンプやシーケンス番号など、インターネット上をＡＶデータを転送する場合に必要となる基本的なパラメータを要素として持つ（なお、詳細は例えばＲＦＣ１８８９に開示されている）。

【００６３】ＲＴＰヘッダが付与された（暗号化された）ＭＰＥＧ４データは、ＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部３０８にて図６のようなＩＰパケットとして、リンク・物理レイヤ処理部３０９を通してインターネット１０３に送出される。

【００６４】図７に、受信装置１０２の内部構成例を示す。

【００６５】図７に示されるように、本実施形態のＭＰＥＧ４配信サーバ１０１は、リンク・物理レイヤ処理部７０１、ＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部７０２、ＲＴＰ基本ヘッダ受信解析部７０４とＭＰＥＧ４拡張ヘッダ受信解析部７０５と暗号拡張ヘッダ受信解析部７０６を含み、ＲＴＰの処理を行うＲＴＰ処理部７０３、データ暗号復号部７０７、ＭＰＥＧ４データデコード部７０８、受信状態解析部７０９、ＲＴＣＰ送信部７１０、認証・鍵交換処理部７１１を備えている。

【００６６】図２のシーケンスの認証や暗号に関する処理（Ｓ２０１～Ｓ２０５までの処理）および暗号鍵更新に関する処理は、認証・鍵交換処理部７１１により行われる。

【００６７】さて、受信装置１０２は、基本的には、ＭＰＥＧ４配信サーバ１０１の逆順に逆変換の処理を行なう。

【００６８】すなわち、まず、インターネット１０３を介して転送されてきたＭＰＥＧ４データ（ＲＴＰヘッダが付与された暗号化データ）は、リンク・物理レイヤ処理部７０１からＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部７０２を経て、ＲＴＰ処理部７０３に入力される。

【００６９】ＲＴＰ処理部３０３では、ＲＴＰ基本ヘッダ受信解析部７０４にてＲＴＰ基本ヘッダが解析され、ＭＰＥＧ４拡張ヘッダ受信解析部７０５にてＭＰＥＧ４拡張ヘッダが解析され、暗号拡張ヘッダ受信解析部３０４にて暗号拡張ヘッダが解析される。また、ＭＰＥＧ４拡張ヘッダ受信解析部７０５からＭＰＥＧ４データデコード部７０８に対して必要な情報が通知され、暗号拡張ヘッダ受信解析部３０４からデータ暗号復号部７０７に対して必要な情報が通知される。

【００７０】そして、ＲＴＰペイロードの暗号化データは、ＲＴＰ処理部７０３からデータ暗号復号部７０７に渡される。データ暗号復号部７０７は、暗号拡張ヘッダ受信解析部３０４からの情報に基づいて復号を行う（暗号を解く）。

【００７１】その際に使用する暗号鍵は、前述の時変の暗号鍵Ｋｃである。すなわち、データ暗号復号部７０７は、暗号拡張ヘッダ受信解析部３０４から通知された暗号拡張ヘッダの暗号化有無フィールドの値を参照することにより受信データが暗号化されていることが分かり（この結果、復号を行うことが決定され）、次にＥｖｅｎ／Ｏｄｄフィールドを参照し、その値を直前に受信した値と比較することによって、インクリメントされている場合には、暗号鍵を更新することが分かる（同一である場合には、暗号鍵は更新されないことになる）。そして、暗号鍵を更新する旨をデータ暗号復号部７０７から認証・鍵交換処理部７１１に伝え、認証・鍵交換処理部７１１では、暗号鍵Ｋｃの更新のタイミングになったので、Ｎｃをインクリメントして前述の関数Ｊにより新たな暗号鍵Ｋｃを生成してデータ暗号復号部７０７に渡す。

【００７２】さらに、復号化された（暗号の解かれた）ＭＰＥＧ４データはデータ暗号復号部７０７からＭＰＥＧ４データデコード部７０８に渡され、ＭＰＥＧ４データデコード部７０８は、ＭＰＥＧ４拡張ヘッダ受信解析

部７０５からの情報に基づいて該ＭＰＥＧ４データをデコードし、ＡＶ出力（例えばアナログ信号）として出力する。

【００７３】ところで、ＲＴＰにはＲＴＣＰ（リアルタイムトランスポート制御プロトコル）なるプロトコルが付随している。このＲＴＣＰは、ＲＴＰのシーケンス番号やタイムスタンプ等を監視し、受信側（本実施形態の場合受信装置１０２）から送信側（本実施形態の場合、ＭＰＥＧ４配信サーバ１０１）に対して、受信状況（パケット廃棄率、パケット配送遅延時間等）を通知する機能がある。これを行なうのが受信装置１０２の受信状態解析部７０９とＲＴＣＰ送信部７１０である。ＭＰＥＧ４配信サーバ１０１は、このＲＴＣＰパケットを、ＲＴＣＰ受信解析部３１０で受信し、必要に応じてＭＰＥＧ４データ生成部３０１にフィードバックをして、最適化を図ることができる。例えば、パケット廃棄が激しい場合は、ネットワークが混雑していると考えて、ＭＰＥＧ４データ生成のビットレートを下げる等のフィードバック制御を行なうようにしてもよい。なお、ＭＰＥＧ４配信サーバ１０１のＲＴＣＰ送信部３０７は、ＲＴＣＰに必要な情報を送信する。

【００７４】さて、前述のように、受信装置１０２では、受信したパケットの暗号拡張ヘッダに含まれるＥｖｅｎ／Ｏｄｄフィールドの監視結果に基づいて、暗号鍵Ｋｃの計算に用いる変数Ｎｃの値を変更する。したがって、送信側から受信側に確実にＮｃの値を更新した旨を伝えることができないと、受信側で暗号鍵Ｋｃの値が計算できないことになり、送信されてくる暗号化データの復号ができないことになる。

【００７５】インターネットは基本的にパケットの廃棄が起こり得るネットワークであるため、Ｅｖｅｎ／Ｏｄｄフィールドの値の意味（インクリメントのタイミング）が正確に通信相手に伝わる保証は無い（特に、Ｅｖｅｎ／Ｏｄｄフィールドのビット長が短いとき）。そこで、受信装置１０２は、「正確なＮｃの値を知りたい」と考えた場合に、送信装置（本実施形態の場合、ＭＰＥＧ４配信サーバ１０１）に対して、Ｎｃの値を要求するオプションを用意するようにしてもよい。

【００７６】ここで、受信装置１０２が「正確なＮｃの値を知りたい」と考える場合の例としては、ＲＴＰ基本ヘッダのタイムスタンプ、あるいはシーケンス番号等で、想定以上に値の「飛び」があった場合に、Ｎｃの値を要求するパケットを送信側に送出する、という方式が考えられる。この「想定値以上の値の飛び」は、「その間にＥｖｅｎ／Ｏｄｄビットの値が変化した可能性がある」ということにつながるためである。これらの処理を行なうのは、ＭＰＥＧ４配信サーバ１０１または受信装置１０２の認証・鍵交換処理部である。このようにすることにより、もし仮にＭＰＥＧ４配信サーバ１０１と受信装置１０２との間でＥｖｅｎ／Ｏｄｄビットの同期が

外れてしまった場合でも、適切な復帰処理を行なうことができるようになる。なお、ＭＰＥＧ４配信サーバ１０１から受信装置１０２にＮｃの値を通知する場合は、対応するＲＴＰや拡張ヘッダ、ペイロードヘッダ等のタイムスタンプやシーケンス番号等の値も同時に通知するようにしてもよい。

【００７７】また、配信されたデータを受信装置（あるいは、受信装置に装着された、ＤＶＤ－ＲＡＭ等の何らかのストレージメディア）に蓄積する場合も考えられる。この場合は、配信されたデータを、暗号化されたデータのままで、対応する暗号鍵Ｋｃとともに蓄積するようにしてもよい。

【００７８】（第２の実施形態）次に、第１の実施形態のパケット形式のバリエーションとなる第２の実施形態について説明する。本実施形態は基本的な構成や動作においては第１の実施形態と同様であるので、本実施形態では第１の実施形態と相違する点を中心に説明する。

【００７９】本実施形態が第１の実施形態と相違する点は、第１の実施形態ではＲＴＰヘッダの拡張ヘッダとして、「暗号拡張ヘッダ」と「ＭＰＥＧ４拡張ヘッダ」を付加したが（図５、図６参照）、本実施形態では、「暗号拡張ヘッダ」はＲＴＰヘッダの拡張ヘッダとして付加するが、「ＭＰＥＧ４拡張ヘッダ」はＲＴＰのペイロードにペイロードヘッダとして搭載する点である（図９、図１０参照）。

【００８０】本実施形態のネットワークの全体構成は第１の実施形態（図１）と同様である。また、処理のシーケンスも第１の実施形態（図２）と同様である。また、暗号拡張ヘッダも第１の実施形態（図４）と同様である。

【００８１】図８に、本実施形態のＭＰＥＧ４配信サーバ１０１の構成例を示す。本実施形態では、ＭＰＥＧ４拡張ヘッダをＲＴＰのペイロードにペイロードヘッダとして搭載するので、ＭＰＥＧ４拡張ヘッダの処理がＲＴＰ処理外となり、図３のＭＰＥＧ４拡張ヘッダ付与部３０５がＲＴＰ処理部３０３内から外へ出され、ＭＰＥＧ４ペイロードヘッダ付与部３１５となっている点が第１の実施形態と相違する点である。

【００８２】図９に、本実施形態において暗号化されたＡＶデータの送信の際に用いられるＲＴＰヘッダの形式を示す。ここで、本実施形態では、ＲＴＰ基本ヘッダには「当該ＲＴＰパケットで転送されるデータの属性（符号化方式等）」を示す「ペイロードタイプ」というフィールドを設けている。本実施形態では、例えば転送されるデータが暗号化されたＭＰＥＧ４である場合に、このフィールドには「暗号化されたＭＰＥＧ４」を示す情報が記述される。受信装置１０２は、このフィールドを参照することにより、転送されているデータが暗号化されたＭＰＥＧ４であることを知ることができる。また、本実施形態では、ＲＴＰ基本ヘッダには「当該ＲＴＰヘッ

ダには、拡張ヘッダが付加されているか否か」を示す「Ｘビット」というフィールドを設けている。本実施形態では、「拡張ヘッダあり」を示すビットが立つことになる。

【００８３】図１０に、本実施形態において、インターネット上を転送されるＩＰパケット全体の形式を示す。

【００８４】図１１に、本実施形態の受信装置１０２の構成例を示す。上記のＭＰＥＧ４配信サーバ１０１と同様にして、ＭＰＥＧ４拡張ヘッダの処理がＲＴＰ処理外となり、図７のＭＰＥＧ４拡張ヘッダ受信解析部７０５がＲＴＰ処理部７０３内から外へ出され、ＭＰＥＧ４ペイロードヘッダ受信解析部７１５となっている点が第１の実施形態と相違する点である。

【００８５】受信装置１０２では、ＲＴＰ基本ヘッダ受信解析部７０４にて、受信したデータが暗号化されたＭＰＥＧ４であることが分かり、また、ＲＴＰヘッダに拡張ヘッダが付加されていることが分かる。そして、暗号拡張ヘッダ受信解析部７０６にて、その拡張ヘッダが暗号拡張ヘッダであることが分かり、また、暗号拡張ヘッダから暗号方式や暗号鍵の更新の有無等を知ることができる。そして、第１の実施形態と同様にデータ暗号復号部７０７にて暗号化ＭＰＥＧ４データを復号し、ＭＰＥＧ４ペイロードヘッダ受信解析部７１５にてＭＰＥＧ４ペイロードヘッダを解析し、さらに第１の実施形態と同様にＭＰＥＧ４データ生成部７０８にて上記解析結果に基づいてＭＰＥＧ４データをデコードして、ＡＶ出力（例えばアナログ信号）として出力する。

【００８６】なお、本実施形態においては、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合には暗号拡張ヘッダの暗号化有無フィールドを参照しないようにしてもよいし、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号拡張ヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【００８７】（第３の実施形態）次に第３の実施形態について説明する。本実施形態では、第２の実施形態と相違する点を中心に説明する。

【００８８】図１２に、本実施形態において暗号化されたＡＶデータの送信の際に用いられるＲＴＰヘッダの形式を示す。また、図１３に、本実施形態において、インターネット上を転送されるＩＰパケット全体の形式を示す。

【００８９】すなわち、第２の実施形態では、ＲＴＰ基本ヘッダ内のペイロードタイプフィールドに、「暗号化されたＭＰＥＧ４」というように、暗号化の有無もしくは暗号化の可能性の有無の通知を含む情報を記述したが、本実施形態では、「ＭＰＥＧ４」のみを記述し、ペイロードタイプフィールドには、暗号化の有無もしくは

暗号化の可能性の有無の通知を含む情報は記述しない。

【００９０】従って、本実施形態では、受信装置１０２は、ペイロードタイプフィールドを参照することにより、受信データがＭＰＥＧ４であることを知ることができるが、暗号化の有無については、ＲＴＰヘッダのＲＴＰ拡張ヘッダ（暗号拡張ヘッダ）を参照して認識することになる。

【００９１】受信装置１０２では、ＲＴＰ基本ヘッダ受信解析部７０４にて、受信したデータがＭＰＥＧ４であることが分かり、また、ＲＴＰヘッダに拡張ヘッダが付加されていることが分かる。そして、暗号拡張ヘッダ受信解析部７０６にて、その拡張ヘッダが暗号拡張ヘッダであることが分かり、また、暗号拡張ヘッダから暗号化の有無や暗号鍵の更新の有無等を知ることができる。以降は、第２の実施形態と同様である。

【００９２】（第４の実施形態）次に第４の実施形態について説明する。本実施形態では、第２の実施形態と相違する点を中心に説明する。

【００９３】本実施形態が第２の実施形態と相違する点は、第２の実施形態では「暗号拡張ヘッダ」はＲＴＰヘッダの拡張ヘッダとして付加し、「ＭＰＥＧ４拡張ヘッダ」はＲＴＰのペイロードにペイロードヘッダとして搭載するが（図９、図１０参照）、本実施形態では、「暗号拡張ヘッダ」と「ＭＰＥＧ４拡張ヘッダ」の両方をＲＴＰのペイロードにペイロードヘッダとして搭載する点である（図１５、図１６参照）。

【００９４】本実施形態のネットワークの全体構成は第２（第１）の実施形態（図１）と同様である。また、処理のシーケンスも第２（第１）の実施形態（図２）と同様である。また、暗号拡張ヘッダ（暗号ペイロードヘッダ）も第２（第１）の実施形態（図４）と同様である。

【００９５】図１４に、本実施形態のＭＰＥＧ４配信サーバ１０１の構成例を示す。本実施形態では、ＭＰＥＧ４拡張ヘッダに加えて暗号拡張ヘッダをもＲＴＰのペイロードにペイロードヘッダとして搭載するので、暗号拡張ヘッダの処理がＲＴＰ処理外となり、図８の暗号拡張ヘッダ付与部３０４もＲＴＰ処理部３０３内から外へ出され、暗号ペイロードヘッダ付与部３１４となっている点が第２の実施形態と相違する点である。

【００９６】図１５に、本実施形態において暗号化されたＡＶデータの送信の際に用いられるＲＴＰヘッダの形式を示す。ペイロードタイプフィールドについては第２の実施形態と同様である。また、Ｘビットフィールドについてはその役割は第２の実施形態と同様であるが、本実施形態では、「拡張ヘッダなし」を示すビットが立つことになる。

【００９７】図１６に、本実施形態において、インターネット上を転送されるＩＰパケット全体の形式を示す。

【００９８】図１７に、本実施形態の受信装置１０２の構成例を示す。上記のＭＰＥＧ４配信サーバ１０１と同

様にして、暗号拡張ヘッダの処理がＲＴＰ処理外となり、図１１の暗号拡張ヘッダ受信解析部７０６がＲＴＰ処理部７０３内から外へ出され、暗号ペイロードヘッダ受信解析部７１６となっている点が第２の実施形態と相違する点である。

【００９９】受信装置１０２では、ＲＴＰ基本ヘッダ受信解析部７０４にて、受信したデータが暗号化されたＭＰＥＧ４であることが分かり、また、ＲＴＰヘッダに拡張ヘッダが付加されていないことが分かる。本実施形態では、以降は、ペイロードに対する処理になる。まず、暗号ペイロード受信解析部７１６にて、そのペイロードヘッダが暗号拡張ヘッダであることが分かり、また、暗号ペイロードヘッダから暗号方式や暗号鍵の更新の有無等を知ることができる。そして、以降は第２の実施形態と同様に、データ暗号復号部７０７にて暗号化ＭＰＥＧ４データを復号し、ＭＰＥＧ４ペイロードヘッダ受信解析部７１５にてＭＰＥＧ４ペイロードヘッダを解析し、さらにＭＰＥＧ４データ生成部７０８にて上記解析結果に基づいてＭＰＥＧ４データをデコードして、ＡＶ出力（例えばアナログ信号）として出力する。

【０１００】なお、本実施形態においても第２の実施形態と同様に、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合には暗号ペイロードヘッダの暗号化有無フィールドを参照しないようにしてもよいし、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号ペイロードヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【０１０１】（第５の実施形態）次に第５の実施形態について説明する。本実施形態では、第２の実施形態と相違する点を中心に説明する。

【０１０２】図１８に、本実施形態において暗号化されたＡＶデータの送信の際に用いられるＲＴＰヘッダの形式を示す。また、図１９に、本実施形態における暗号拡張ヘッダの形式を示す。また、図２０に、本実施形態において、インターネット上を転送されるＩＰパケット全体の形式を示す。

【０１０３】すなわち、第２の実施形態では、ＲＴＰ基本ヘッダ内のペイロードタイプフィールドに、「暗号化されたＭＰＥＧ４」というように、その暗号化データの属性（符号化方式等）の通知を含む情報を記述したが（図９、図１１参照）、本実施形態では、「暗号化データ」というように、ペイロードタイプフィールドには、「暗号化データ」という暗号化有りを通知する情報のみを記述する（図１８、図２０参照）。そして、暗号拡張ヘッダをＲＴＰヘッダの拡張ヘッダとして付加し、ＭＰＥＧ４拡張ヘッダをＲＴＰのペイロードにペイロードヘッダとして搭載する点は第２の実施形態と同様である

が、本実施形態では、上記の暗号化データの属性（符号化方式等）については暗号拡張ヘッダ内に記述するようにしている（図４、図１９参照）。

【０１０４】本実施形態のネットワークの全体構成は第２（第１）の実施形態（図１）と同様である。また、処理のシーケンスも第２（第１）の実施形態（図２）と同様である。また、ＭＰＥＧ４配信サーバおよび受信装置１０２の内部構造も第２の実施形態（図８，図１１）と同様である。

【０１０５】図１８に示すように、本実施形態では、ＲＴＰ基本ヘッダのペイロードタイプフィールドには「暗号化されたデータ」を示す値が記述される。受信装置１０２は、このフィールドを参照することにより、転送されているデータが暗号化されたデータであることを知ることができる。また、本実施形態では、Ｘビットフィールドには「拡張ヘッダあり」を示すビットが立つことになる。

【０１０６】図１９に示すように、本実施形態では、暗号拡張ヘッダには、ペイロードタイプフィールドを設ける。ペイロードタイプフィールドには、ペイロードに入るデータの種別（本実施形態の場合、ＭＰＥＧ４）を示す情報が記述される。受信装置１０２は、このフィールドを参照することにより、転送されているデータの種別を知ることができる。

【０１０７】受信装置１０２では、ＲＴＰ基本ヘッダ受信解析部７０４にて、受信したデータが暗号化されたデータであることが分かり、また、ＲＴＰヘッダに拡張ヘッダが付加されていることが分かる。そして、暗号拡張ヘッダ受信解析部７０６にて、その拡張ヘッダが暗号拡張ヘッダであることが分かり、また、暗号拡張ヘッダから暗号方式や暗号鍵の更新の有無等およびペイロードに入るデータの種別を知ることができる。そして、第２の実施形態と同様に、データ暗号復号部７０７にて暗号化ＭＰＥＧ４データを復号し、ＭＰＥＧ４ペイロードヘッダ受信解析部７１５にてＭＰＥＧ４ペイロードヘッダを解析し、さらにＭＰＥＧ４データ生成部７０８にて上記解析結果に基づいてＭＰＥＧ４データをデコードして、ＡＶ出力（例えばアナログ信号）として出力する。

【０１０８】なお、本実施形態においても第２の実施形態と同様に、ＲＴＰ基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合には暗号拡張ヘッダの暗号化有無フィールドを参照しないようにしてもよいし、ＲＴＰ基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号拡張ヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【０１０９】（第６の実施形態）次に第６の実施形態について説明する。本実施形態では、第４の実施形態と相

違する点を中心に説明する。

【０１１０】図２１に、本実施形態において暗号化されたＡＶデータの送信の際に用いられるＲＴＰヘッダの形式を示す。また、本実施形態における暗号拡張ヘッダの形式は図１９と同様である。また、図２２に、本実施形態において、インターネット上を転送されるＩＰパケット全体の形式を示す。

【０１１１】すなわち、「暗号拡張ヘッダ」と「ＭＰＥＧ４拡張ヘッダ」の両方をＲＴＰのペイロードにペイロードヘッダとして搭載する点は第４の実施形態と同様であるが（図１５、図１６参照）、第４の実施形態では、ＲＴＰ基本ヘッダ内のペイロードタイプフィールドに、「暗号化されたＭＰＥＧ４」というように、その暗号化データの属性（符号化方式等）の通知を含む情報を記述するのに対し、本実施形態では、「暗号化データ」というように、ペイロードタイプフィールドには、「暗号化データ」という暗号化有りを通知する情報のみを記述する（図２１、図２２参照）。そして、暗号拡張ヘッダをＲＴＰヘッダの拡張ヘッダとして付加し、ＭＰＥＧ４拡張ヘッダをＲＴＰのペイロードにペイロードヘッダとして搭載する点は第２の実施形態と同様であるが、本実施形態では、上記の暗号化データの属性（符号化方式等）については暗号拡張ヘッダ内に記述するようにしている（図４、図１９参照）。

【０１１２】本実施形態のネットワークの全体構成は第４（第１）の実施形態（図１）と同様である。また、処理のシーケンスも第４（第１）の実施形態（図２）と同様である。また、ＭＰＥＧ４配信サーバおよび受信装置１０２の内部構造も第４の実施形態（図１４，図１７）と同様である。

【０１１３】図２１に示されるように、本実施形態では、ＲＴＰ基本ヘッダのペイロードタイプフィールドには「暗号化されたデータ」を示す値が入る。受信装置１０２は、このフィールドを見ることにより、転送されているデータが暗号化されたものであることを知ることができる。また、Ｘビットには「拡張ヘッダ無し」を示すビットが立つ。また、第４の実施形態と同様に、暗号拡張ヘッダのペイロードタイプフィールドに、ペイロードに入るデータの種別（本実施形態の場合、ＭＰＥＧ４）を示す情報が記述される。

【０１１４】受信装置１０２では、ＲＴＰ基本ヘッダ受信解析部７０４にて、受信したデータが暗号化されたデータであることが分かり、また、ＲＴＰヘッダに拡張ヘッダが付加されていないことが分かる。本実施形態では、以降は、ペイロードに対する処理になる。まず、暗号ペイロード受信解析部７１６にて、そのペイロードヘッダが暗号拡張ヘッダであることが分かり、また、暗号ペイロードヘッダから暗号方式や暗号鍵の更新の有無等およびペイロードに入るデータの種別を知ることができる。そして、以降は第４の実施形態と同様に、データ暗

号復号部７０７にて暗号化ＭＰＥＧ４データを復号し、ＭＰＥＧ４ペイロードヘッダ受信解析部７１５にてＭＰＥＧ４ペイロードヘッダを解析し、さらにＭＰＥＧ４データ生成部７０８にて上記解析結果に基づいてＭＰＥＧ４データをデコードして、ＡＶ出力（例えばアナログ信号）として出力する。

【０１１５】なお、本実施形態においても第４の実施形態と同様に、ＲＴＰ基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合には暗号拡張ヘッダの暗号化有無フィールドを参照しないようにしてもよいし、ＲＴＰ基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号拡張ヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【０１１６】（第７の実施形態）第１～第６の実施形態では、本発明をトランスポートプロトコルとしてＲＴＰを使用するシステムに適用した場合について説明してきたが、本発明は、それ以外のプロトコルを使用するシステムに対しても適用可能である。

【０１１７】第７の実施形態では、トランスポートプロトコルとしてＲＴＰを使うのではなく、ＭＰＥＧ４のデータ配信を、ＷＷＷサーバとＷｅｂブラウザ間のプロトコルであるＨＴＴＰ（ハイパーテキストトランスファープロトコル）（およびＴＣＰ）を使って行なう場合の例について説明する。

【０１１８】図２３に、本実施形態における情報配信システムの構成例を示す。図２３では、インターネット６１０３に本実施形態に係るＭＰＥＧ４配信サーバ６１０１が接続され、ＬＡＮ６１０５に本実施形態に係る受信装置６１０２が接続されており、ＬＡＮ６１０５はプロキシサーバ６１０４を介してインターネット６１０３に接続されている。そして、受信装置６１０２は、ＬＡＮ６１０５、プロキシサーバ６１０４、インターネット６１０３を介してＭＰＥＧ４配信サーバ６１０１との間でＭＰＥＧ４のＡＶストリームの秘匿通信を行うものである。もちろん、インターネット６１０３には他のＭＰＥＧ４配信サーバあるいはその他の種類の機器が接続されていてもかまわないし、ＬＡＮ６１０６には他の受信装置あるいはその他の種類の機器が接続されていてもかまわない。

【０１１９】また、本実施形態では、データの種別をＭＰＥＧ４として説明するが、もちろん他の種別のデータにも本発明は適用可能である。

【０１２０】さて、図２３において、各々の装置はＩＰをサポートしている装置であるが、インターネット６１０３とＬＡＮ６１０５との間にＨＴＴＰプロキシサーバ６１０４が存在しているため、ＬＡＮ６１０５上のＩＰアドレスは、グローバルＩＰアドレスであっても、プラ

イベートＩＰアドレスであってもよい。ここで、プロキシサーバとは、インターネットとイントラネットの間に入り、ＨＴＴＰ（その他のプロトコルでもよい）を一度終端すると共に、プロキシサーバの両端のＨＴＴＰセッションを結び付けて、実質上受信装置（Ｗｅｂブラウザ）から要求のあったＨＴＴＰコンテンツを配信サーバ（WWWサーバ）に対して（あるいは逆方向に）データを配信できるようにするためのサーバである。なお、プロキシサーバの詳細については、例えばｈｔｔｐ：／／ｓｑｕｉｄ．ｎｌａｎｒ．ｎｅｔ／Ｓｑｕｉｄ／等に開示されている。本実施形態においては、ＭＰＥＧ４配信サーバはWWWサーバ、受信装置はＷｅｂブラウザであってもよい。

【０１２１】図２４に、認証手続きや認証鍵の交換の手続きあるいは暗号化されたデータ等のシーケンスの一例を示す。受信装置６１０２とＭＰＥＧ４配信サーバ６１０１との間にプロキシサーバ６１０２が入っているために実際のメッセージ（ＨＴＴＰメッセージとして転送される）は一度プロキシサーバ６１０２にて中継される点がこれまでの第１～第６の実施形態（図２）と相違するだけであり、それ以外の点は第１～第６の実施形態と同様の手続きである。

【０１２２】さて、ＭＰＥＧ４配信サーバ６１０１、受信装置６１０２、パケットの形式などについては、例えば、前述した第１～第６の実施形態において対応するものについて、トランスポートプロトコルに依存する部分をＨＴＴＰプロトコルに対応するように修正すれば、ＨＴＴＰプロトコルに対応したＭＰＥＧ４配信サーバ６１０１、受信装置６１０２、パケットの形式などを構成することができる。以下では、「暗号拡張ヘッダ」は拡張ヘッダとして付加するが「ＭＰＥＧ４拡張ヘッダ」はペイロードにペイロードヘッダとして搭載する構成（第２の実施形態参照）に対応する構成を例にとって説明する。

【０１２３】図２５に、ＭＰＥＧ４配信サーバ６１０１の内部構成例を示す。

【０１２４】図２５に示されるように、本実施形態のＭＰＥＧ４配信サーバ６１０１は、ＭＰＥＧ４データ生成部６３０１、データ暗号部６３０２、ＭＰＥＧ４ペイロードヘッダ付与部６３０５、暗号ヘッダ付与部６３０４とＭＩＭＥヘッダ付与部６３０６を含むＨＴＴＰ処理部６３０３、ＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部６３０８、リンク・物理レイヤ処理部６３０９、認証・鍵交換処理部６３１１を備えている。

【０１２５】図２４のシーケンスの認証や暗号に関する処理（Ｓ６２０１～Ｓ６２０５までの処理）および暗号鍵更新に関する処理は、認証・鍵交換処理部６３１１により行われる。

【０１２６】ＨＴＴＰ処理部６３０３がこれまでの実施形態のＲＴＰ処理部に相当し、ＭＩＭＥヘッダ付与部６３０６がこれまでの実施形態のＲＴＰ基本ヘッダ付与部に相当する。

【０１２７】図２６に、インターネット（及びＬＡＮ）上を転送されるＩＰパケットを示し、図２７に、ＭＩＭＥ基本ヘッダおよび暗号拡張ヘッダの詳細を示す。

【０１２８】本実施形態では、暗号拡張ヘッダは、ＭＩＭＥの一つのパートとして転送される。このため、暗号拡張ヘッダは、ＭＩＭＥの“Ｃｏｎｔｅｎｔ－Ｔｙｐｅ”に、それが暗号拡張ヘッダである旨を示す情報が記載される。また、ＭＰＥＧ４拡張ヘッダはペイロードヘッダとして暗号化されたＭＰＥＧ４データとともにＭＩＭＥの一つのパートとして転送される。ＭＰＥＧ４拡張ヘッダの付加された暗号化ＭＰＥＧ４データは、ＭＩＭＥの“Ｃｏｎｔｅｎｔ－Ｔｙｐｅ”に、それがＭＰＥＧ４データであるである旨を示す情報が記載される。なお、ＭＩＭＥの詳細については例えばＲＦＣ２０４５等に開示されている。

【０１２９】暗号拡張ヘッダの形式は、第１の実施形態と同様である。

【０１３０】図２８に、受信装置６１０２の内部構成例を示す。

【０１３１】図２８に示されるように、本実施形態のＭＰＥＧ４配信サーバ６１０１は、リンク・物理レイヤ処理部６７０１、ＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部６７０２、ＭＩＭＥヘッダ解析部６７０４と暗号ヘッダ解析部６７０６を含むＨＴＴＰ処理部６７０３、ＭＰＥＧ４ペイロードヘッダ解析部６７０５、データ暗号復号部６７０７、ＭＰＥＧ４データデコード部６７０８、認証・鍵交換処理部６７１１を備えている。

【０１３２】図２４のシーケンスの認証や暗号に関する処理（Ｓ６２０１～Ｓ６２０５までの処理）および暗号鍵更新に関する処理は、認証・鍵交換処理部６７１１により行われる。

【０１３３】ＨＴＴＰ処理部６７０３がこれまでの実施形態のＲＴＰ処理部に相当し、ＭＩＭＥヘッダ解析部６３０６がこれまでの実施形態のＲＴＰ基本ヘッダ受信解析部に相当する。

【０１３４】ＭＰＥＧ４配信サーバ６１０１においては、入力されたＡＶ入力（例えばアナログ信号）は、ＭＰＥＧ４データ生成部６３０１にてＭＰＥＧ４のデータに圧縮される。また、ＭＰＥＧ４データ生成部６３０１からＭＰＥＧ４ペイロードヘッダ付与部６３０５に対して必要な情報が通知される。

【０１３５】次に、ＭＰＥＧ４データ生成部３０１から出力されたＭＰＥＧ４データをデータ暗号部６３０２が暗号化する。その際に使用する暗号鍵は、前述の時変の暗号鍵Ｋｃである。また、データ暗号部６３０２から暗号ヘッダ付与部６３０４に対して必要な情報が通知される。

【０１３６】次に、ＨＴＴＰ処理部６３０３では、暗号

ヘッダ付与部６３０４にて暗号拡張ヘッダが付加され、ＭＩＭＥヘッダ付与部６０３６にてＭＩＭＥヘッダが付加される。

【０１３７】そして、ＭＩＭＥヘッダが付与された暗号化されたＭＰＥＧ４データは、ＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部６３０８にて図２６のようなＩＰパケットとして、リンク・物理レイヤ処理部６３０９を通してインターネット６１０３に送出される。

【０１３８】受信装置６１０２においては、ＭＩＭＥヘッダ解析部６７０４にて、受信したデータが暗号化された可能性のあるＭＰＥＧ４であることが分かり、また、ＭＩＭＥの一つのパートとして暗号拡張ヘッダが付加されていることが分かる。そして、暗号ヘッダ解析部６７０６にて、その暗号拡張ヘッダから暗号化の有無、暗号方式や暗号鍵の更新の有無等を知ることができる。そして、第２の実施形態と同様に、データ暗号復号部６７０７にて暗号化ＭＰＥＧ４データを復号し、ＭＰＥＧ４ペイロードヘッダ解析部６７１５にてＭＰＥＧ４ペイロードヘッダ（これまでの実施形態のＭＰＥＧ４ペイロードヘッダと同様）を解析し、さらにＭＰＥＧ４データ生成部６７０８にて上記解析結果に基づいてＭＰＥＧ４データをデコードして、ＡＶ出力（例えばアナログ信号）として出力する。

【０１３９】なお、ここでは、「暗号拡張ヘッダ」は拡張ヘッダとして付加するが「ＭＰＥＧ４拡張ヘッダ」はペイロードにペイロードヘッダとして搭載する構成を示したが、例えば、「暗号拡張ヘッダ」および「ＭＰＥＧ４拡張ヘッダ」を拡張ヘッダとして付加する構成や、「暗号拡張ヘッダ」および「ＭＰＥＧ４拡張ヘッダ」をペイロードにペイロードヘッダとして搭載する構成など、他の構成も可能である。

【０１４０】ところで、第１～第７の実施形態では、送信側から受信側へ暗号鍵Ｋｃの生成のための変数Ｎｃの値の更新を通知するために、暗号拡張ヘッダ（暗号ペイロードヘッダ）のＥｖｅｎ／Ｏｄｄフィールドを用いたが、その代わりに、Ｎｃの値を送信するようにしてもよい。この場合に、Ｎｃの値は、１づつインクリメントするのではなく、その都度ランダムに発生するようにしてもよい。また、Ｎｃの値をパケット毎に変化させるようにしてもよい。

【０１４１】また、第１～第７の実施形態では、転送プロトコルとしてＲＴＰやＨＴＴＰを用いてきたが、もちろんその他のプロトコルを用いてもよい。また、適用できるネットワークもインターネットに限定されるものではない。また、前述したように、転送するデータの種別もＭＰＥＧ４に限定されるものではない。

【０１４２】また、第２、第３、第５の実施形態では、データ暗号部３０２／データ暗号復号部７０７をＲＴＰ処理部３０３，３０７の外部に設けたが、それらをＲＴＰ処理部３０３，３０７の内部に設けるようにしてもよい。

【０１４３】（第８の実施形態）次に第８の実施形態について説明する。

【０１４４】第１～第７の実施形態では、図２に例示したシーケンスを用いて説明したが、もちろん本発明は、その他のシーケンスについても適用可能である。

【０１４５】以下では、その他のシーケンスを用いた例について説明する。なお、ここでは、受信装置がＭＰＥＧ４配信サーバから配信されたＭＰＥＧ４データを蓄積する場合を考える。

【０１４６】本実施形態の情報配信システムの構成例は図１と同様とする。図１では、インターネット１０３に本実施形態に係るＭＰＥＧ４配信サーバ１０１および受信装置１０２が接続されており、インターネット１０３を通してＭＰＥＧ４配信サーバ１０１と受信装置１０２との間でＭＰＥＧ４のＡＶストリームの秘匿通信を行うものである。もちろん、インターネット１０３には他のＭＰＥＧ４配信サーバや受信装置あるいはその他の種類の機器が接続されていてもかまわない。

【０１４７】また、本実施形態でもデータの種別をＭＰＥＧ４として説明するが、もちろん他の種別のデータにも本発明は適用可能である。

【０１４８】このＭＰＥＧ４配信サーバ１０１は、受信装置１０２に対して、ＭＰＥＧ４データの配信を行う。ＭＰＥＧ４データは、ファイル転送の形ではなく、ストリーム配信の形をとる。このとき、著作権保護の対象とするＭＰＥＧ４データは、暗号化した状態で配信する。その際、配信に先立って、ＭＰＥＧ４配信サーバ１０１と受信装置１０２との間で、認証手続きや認証鍵の交換の手続きなどを行う。

【０１４９】このときのシーケンスの一例を図２９に示す。

【０１５０】なお、図２９は、いわゆるコンテンツレイヤの暗号化や認証について示したものであり、ＩＰレイヤあるいはトランスポートレイヤ等のレイヤにおけるセキュリティやそれらレイヤでの認証手続き等に関しては省略してあり、またコンテンツレイヤで先立って行われる課金などの手続きも省略してある（課金処理や他レイヤのでの認証／暗号処理が行われない場合もあり得る）。

【０１５１】第１の実施形態と同様に、ＭＰＥＧ４配信サーバ１０１と受信装置１０２は、認証と、証書（機器証明）の交換を行う（Ｓ７２０１，Ｓ７２０２）。

【０１５２】ここで、ＭＰＥＧ４配信サーバ１０１は、コンテンツ（送信するＡＶデータ）を復号するための暗号鍵Ｋｃを受信装置１０２に通知する必要があるが、受信装置１０２にて無制限にコンテンツの不正コピーを行なうことができないように、以下のような方策を講じる。すなわち、受信装置１０２のストレージメディア（例えばＤＶＤ－ＲＡＭ）に記録するとき、ＡＶデータ

は暗号化された状態で記録する。また、そのストレージメディア上のデータを再生する場合も、それが本来そのストレージメディアに記録されるべくしてされたものであることを確認し、そのストレージメディアそのものでないと再生できないようにする。すなわち、この場合、そのストレージメディアから、別のストレージメディア（例えば別のＤＶＤ－ＲＡＭ）にコピー（デジタルダビング）を行なった場合には、コピーメディアでは再生ができないようにする。

【０１５３】そのために、受信装置１０２からＭＰＥＧ４配信サーバ１０１に、受信装置１０２で用いるストレージメディアのＩＤ（通し番号）ＭＩＤを通知し（ステップＳ７２０３）、ＭＰＥＧ４配信サーバ１０１では、このＭＩＤの値を用いて暗号鍵Ｋｃを暗号化して、受信装置１０２に通知する（ステップＳ７２０４）。より具体的には、予め定められた関数ｇを用いてＷ＝ｇ（ＭＩＤ）の形で暗号鍵Ｗを生成し、この暗号鍵Ｗを用いて暗号鍵Ｋｃを暗号化し（この暗号鍵Ｗで暗号化された暗号鍵Ｋｃを［Ｋｃ］ｗと記述する）、［Ｋｃ］ｗを送信する。ここで、ＭＩＤの値は、ストレージメディア毎に異なる値であるとし、ＲＯＭ等の書き換え不可能な領域に持っているものとする。

【０１５４】上記の［Ｋｃ］ｗを受信した受信装置１０２は、ＭＰＥＧ４配信サーバ１０１と同一の関数ｇを用いてＷ＝ｇ（ＭＩＤ）の形で暗号鍵Ｗを生成し、この暗号鍵Ｗを用いて［Ｋｃ］ｗを復号して暗号鍵Ｋｃを求める。

【０１５５】以降は、ＭＰＥＧ４配信サーバ１０１では、ＡＶデータからＭＰＥＧ４データを生成し、上記のようにして共有された暗号鍵ＫｃでこのＭＰＥＧ４データを暗号化し、暗号化ＭＰＥＧ４データを、ＡＶデータが受信装置１０２に対して送信する（ステップＳ７２０６）。

【０１５６】一方、受信装置１０２は、受信した暗号化された暗号化されたＭＰＥＧ４データを、上記のようにして求めた暗号鍵ｋｃで復号し、該ＭＰＥＧ４データをデコードして、ＡＶ出力として出力する。

【０１５７】また、本実施形態では、受信装置１０２は、ＡＶデータ（暗号鍵Ｋｃで暗号化されたＭＰＥＧ４データ）を受信すると同時にもしくは一旦バッファ等に蓄積した後に、受信したＡＶデータを暗号鍵Ｋｃで暗号化されたＭＰＥＧ４データの形で、［Ｋｃ］ｗの値とともに、先のＭＩＤを持つストレージメディアに記録する機能を有する。

【０１５８】この場合、この適正なストレージメディアに記録されたＡＶデータ（暗号鍵Ｋｃで暗号化されたＭＰＥＧ４データ）を再生する装置（受信装置１０２であってもよいし、他の装置であってもよい）は、まず、該ストレージメディアから［Ｋｃ］ｗの値およびＭＩＤを読み出し、Ｗ＝ｇ（ＭＩＤ）の形で暗号鍵Ｗを生成し、

この暗号鍵Ｗで［Ｋｃ］ｗを復号して暗号鍵Ｋｃを求める。そして、ストレージメディアに記録されたＡＶデータ（暗号鍵Ｋｃで暗号化されたＭＰＥＧ４データ）を読み出して、この暗号鍵Ｋｃで復号した後にＭＰＥＧ４データをデコードする。

【０１５９】一方、あるＭＩＤ１を持つストレージメディアに記録されたＡＶデータ（暗号鍵Ｋｃで暗号化されたＭＰＥＧ４データ）を、異なるＭＩＤ２を持つストレージメディアにコピーした場合、このコピー先のストレージメディアに記録されたデータを再生する装置においては、もとの適正なストレージメディアのＭＩＤが得られないので、Ｗを生成できず、よって記録されている［Ｋｃ］ｗから暗号鍵Ｋｃを求めることができず、この結果、記録された暗号化データを復号することができないことになる。すなわち、適正なＫｃ、Ｗ、［Ｋｃ］ｗを、Ｋｃ１、Ｗ１＝ｇ（ＭＩＤ１）、［Ｋｃ］ｗ１とすると、該ストレージメディアから読み出したＭＩＤはＭＩＤ２であり、これをもとに生成した暗号鍵Ｗは、Ｗ２＝ｇ（ＭＩＤ２）となるので、該ストレージメディアから読み出した［Ｋｃ］ｗ１をＷ２で復号すると、Ｋｃとは異なる値が求まる（これをＫｃ’とする）。したがって、Ｋｃで暗号化されたデータ［Ｄａｔａ］ＫｃをＫｃ’で復号しても、もとのデータＤａｔａとは異なるＤａｔａ’が生成され、もとのデータＤａｔａを得ることはできない。

【０１６０】このように、受信したＡＶデータ（暗号鍵Ｋｃで暗号化されたＭＰＥＧ４データ）を他のストレージメディアメディアにコピーしても、そのストレージメディアのＭＩＤの値が異なるため、当該ＡＶデータを再生不能とすることができ、不正な複製を未然に防止することができる。

【０１６１】なお、本実施形態において、ＲＴＰヘッダ、暗号拡張（ペイロード）ヘッダ、ＭＰＥＧ４拡張（ペイロード）ヘッダ等に関しては、第１～第７の実施形態と同様の構成でよい。

【０１６２】以上の各実施形態では符号化方式としてＭＰＥＧ４を例にとって説明したが、もちろん他の符号化方式も使用可能である。この場合には、各実施形態の装置の該当する構成部分（例えば、ＭＰＥＧ４データ生成部、ＭＰＥＧ４拡張ヘッダ付与部、ＭＰＥＧ４データデコード部、ＭＰＥＧ４拡張ヘッダ受信解析部等）、拡張ヘッダ（ＭＰＥＧ４拡張ヘッダ、ＭＰＥＧ４ペイロードヘッダ）、ペイロードタイプの記述等を、それぞれの符号化方式に応じて修正すればよい。また、各実施形態の配信サーバは、必要に応じて、コンテンツを暗号化しないで送信するようにすることも可能である。すなわち、暗号化の有無に応じて、暗号化有無フィールドやペイロードタイプ等の記述内容を適宜決定すればよい。受信装置側も、受信したパケットのヘッダから暗号化の有無を調べることにより、暗号化の有無に応じて復号化処理を

制御すればよい。

【０１６３】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【０１６４】また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【０１６５】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１６６】

【発明の効果】本発明によれば、コピープロテクション技術をＩＥＥＥ１３９４のみならずインターネット等のネットワーク上のコンテンツ流通にも拡張することが可能となる。

【図面の簡単な説明】

【図１】本発明の第１～第６の実施形態に係るネットワークの構成例を示す図

【図２】本発明の第１～第６の実施形態に係るシーケンスの例を示す図

【図３】本発明の第１の実施形態に係るＭＰＥＧ配信サーバの構成例を示す図

【図４】暗号拡張ヘッダのフォーマットの第１の例を示す図

【図５】ＲＴＰ処理部で付与されるヘッダのフォーマットの第１の例を示す図

【図６】転送されるＩＰパケットのフォーマットの第１の例を示す図

【図７】本発明の第１の実施形態に係る受信装置の構成例を示す図

【図８】本発明の第２、第３、第５の実施形態に係るＭＰＥＧ配信サーバの構成例を示す図

【図９】ＲＴＰ処理部で付与されるヘッダのフォーマットの第２の例を示す図

【図１０】転送されるＩＰパケットのフォーマットの第２の例を示す図

【図１１】本発明の第２、第３、第５の実施形態に係る受信装置の構成例を示す図

【図１２】ＲＴＰ処理部で付与されるヘッダのフォーマットの第３の例を示す図

【図１３】転送されるＩＰパケットのフォーマットの第３の例を示す図

【図１４】本発明の第４、第６の実施形態に係るＭＰＥＧ配信サーバの構成例を示す図

【図１５】ＲＴＰ処理部で付与されるヘッダのフォーマットの第４の例を示す図

【図１６】転送されるＩＰパケットのフォーマットの第４の例を示す図

【図１７】本発明の第４、第６の実施形態に係る受信装置の構成例を示す図

【図１８】ＲＴＰ処理部で付与されるヘッダのフォーマットの第５の例を示す図

【図１９】暗号拡張ヘッダのフォーマットの第２の例を示す図

【図２０】転送されるＩＰパケットのフォーマットの第５の例を示す図

【図２１】ＲＴＰ処理部で付与されるヘッダのフォーマットの第６の例を示す図

【図２２】転送されるＩＰパケットのフォーマットの第６の例を示す図

【図２３】本発明の第７の実施形態に係るネットワークの構成例を示す図

【図２４】本発明の第７の実施形態に係るシーケンスの例を示す図

【図２５】本発明の第７の実施形態に係るＭＰＥＧ配信サーバの構成例を示す図

【図２６】転送されるＩＰパケットのフォーマットの第７の例を示す図

【図２７】ＲＴＰ処理部で付与されるヘッダのフォーマットの第７の例を示す図

【図２８】本発明の第７の実施形態に係る受信装置の構成例を示す図

【図２９】本発明の第８の実施形態に係るシーケンスの例を示す図

【符号の説明】

１０１，６１０１…ＭＰＥＧ４配信サーバ

１０２，６１０２…受信装置

１０３，６１０３…インターネット

６１０４…プロキシサーバ

６１０５…ＬＡＮ

３０１，６３０１…ＭＰＥＧ４データ生成部

３０２，６３０２…データ暗号部

３０３，７０３…ＲＴＰ処理部

３０４…暗号拡張ヘッダ付与部

３１４…暗号ペイロードヘッダ付与部

３０５…ＭＰＥＧ４拡張ヘッダ付与部

３１５，６３０５…ＭＰＥＧ４ペイロードヘッダ付与部

３０６…ＲＴＰ基本ヘッダ付与部

３０７…ＲＴＣＰ送信部

３０８，７０２，６３０８，６７０２…ＴＣＰ／ＩＰ及びＵＤＰ／ＩＰ処理部

３０９，７０１，６３０９，６７０１…リンク・物理レイヤ処理部

３１０…ＲＴＣＰ受信解析部

３１１，７１１，６３１１，６７１１…認証・鍵交換処理部

７０４…ＲＴＰ基本ヘッダ受信解析部

７０５…ＭＰＥＧ４拡張ヘッダ受信解析部

33

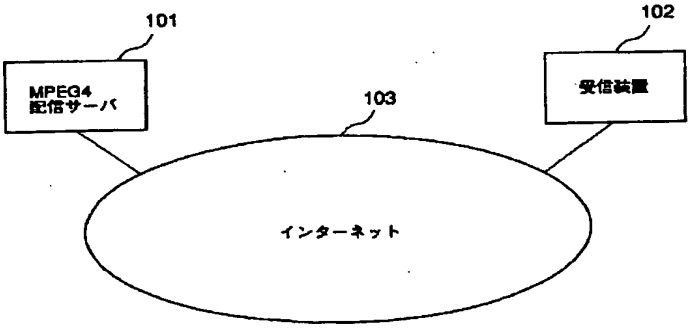
７１５…ＭＰＥＧ４ペイロードヘッダ受信解析部
７０６…暗号拡張ヘッダ受信解析部
７１６…暗号ペイロードヘッダ受信解析部
７０７，６７０７…データ暗号復号部
７０８，６７０８…ＭＰＥＧ４データデコード部
７０９…受信状態解析部
７１０…ＲＴＣＰ送信部

34

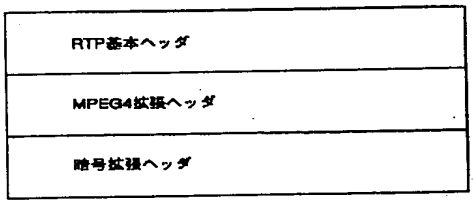
＊６３０３，６７０３…ＨＴＴＰ処理部
６３０４…暗号ヘッダ付与部
６３０６…ＭＩＭＥヘッダ付与部
６７０４…ＭＩＭＥヘッダ解析部
６７０５…ＭＰＥＧ４ペイロードヘッダ解析部
６７０６…暗号ヘッダ解析部

＊

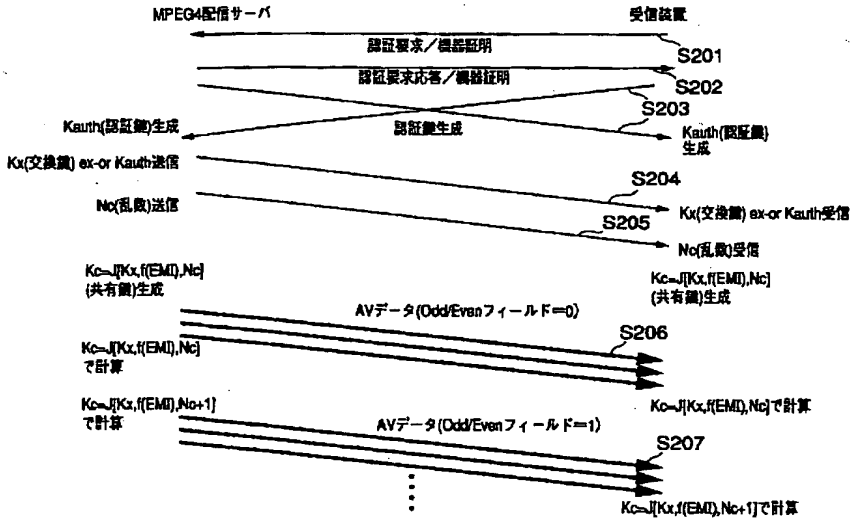
【図１】



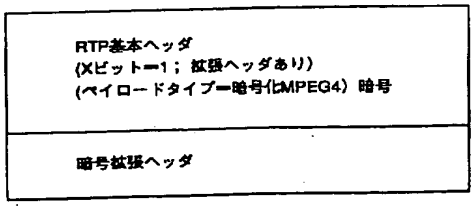
【図５】



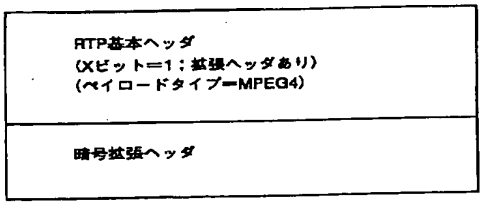
【図２】



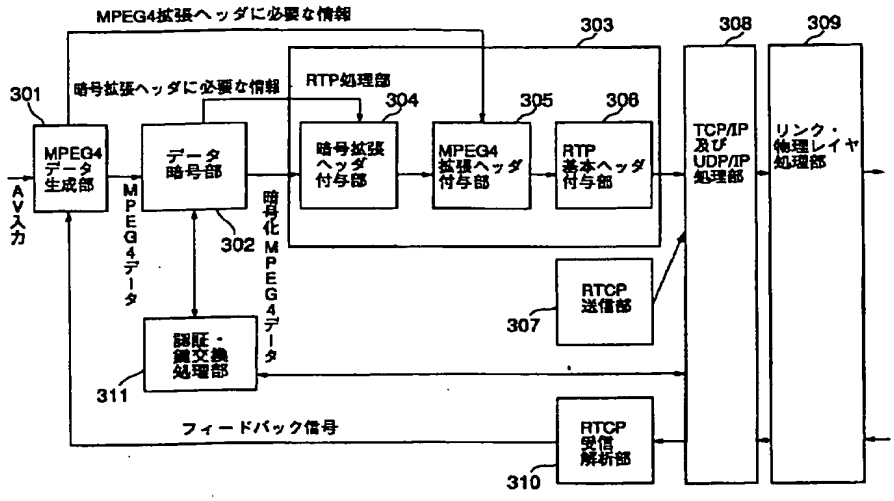
【図９】



【図１２】



【図３】



【図４】

	拡張ヘッダ種別フィールド（種別＝暗号拡張ヘッダ）
8ビット	暗号化有無フィールド（暗号あり）
8ビット	暗号方式表示フィールド（暗号方式＝M6）
8ビット	暗号モードインジケータ（EMI）フィールド
8ビット	Even/Oddフィールド

【図６】

IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ
	MPEG4拡張ヘッダ
	暗号拡張ヘッダ
[MPEG4データ]Kc (暗号化されたMEG4データ)	

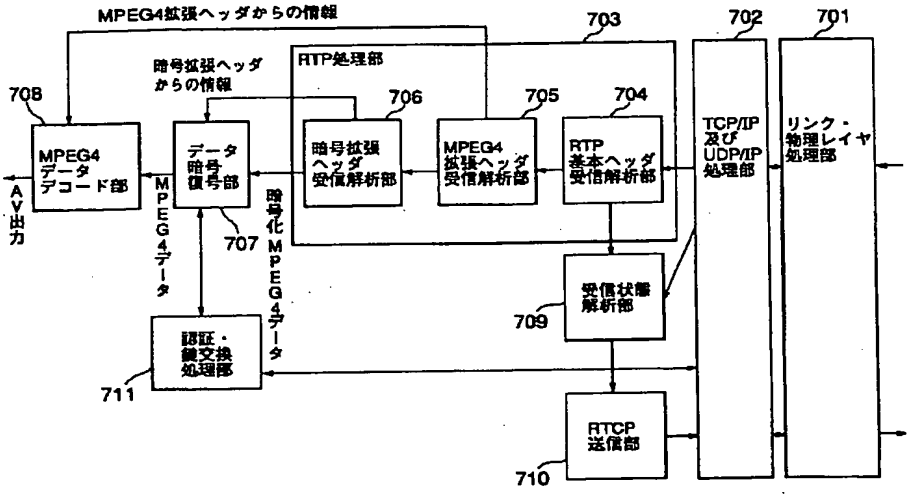
【図１０】

IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ（PT＝暗号化MPEG4）
	暗号拡張ヘッダ
RTPペイロード	MPEG4ペイロードヘッダ
	[MPEG4データ]Kc (暗号化されたMEG4データ)

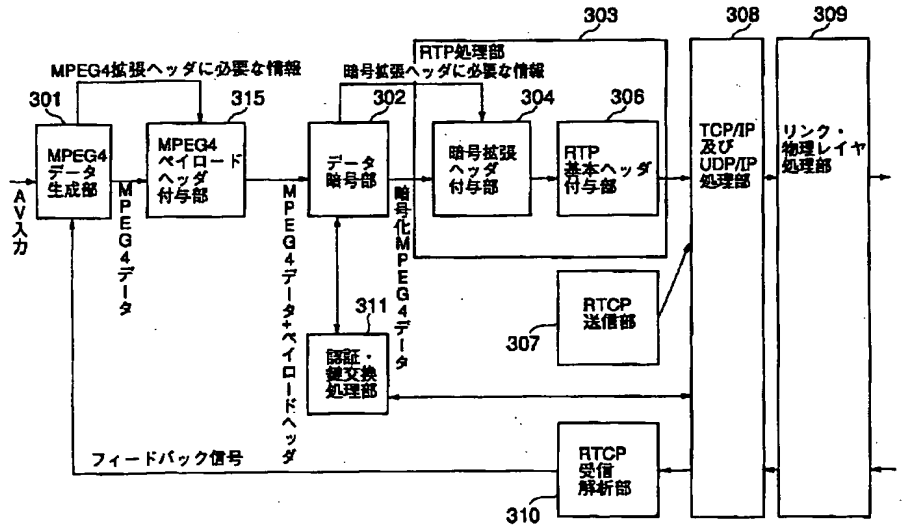
【図１５】

RTP基本ヘッダ
（Xビット＝0；拡張ヘッダ無し）
（ペイロードタイプ＝暗号化MPEG4）

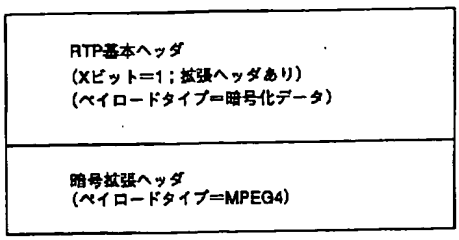
【図７】


MPEG4拡張ヘッダからの情報
703
702
701
RTP処理部
暗号拡張ヘッダ
からの情報
708
706
705
704
MPEG4
データ
デコード部
データ
暗号
復号部
暗号拡張
ヘッダ
受信解析部
MPEG4
拡張ヘッダ
受信解析部
RTP
基本ヘッダ
受信解析部
TCP/IP
及び
UDP/IP
処理部
リンク・
物理レイヤ
処理部
AV出力
MPEG4データ
707
暗号化MPEG4データ
受信状態
解析部
709
認証・
鍵交換
処理部
711
RTCP
送信部
710

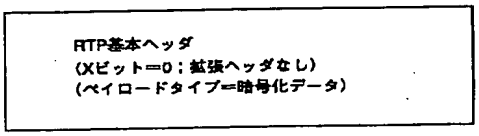
【図８】


303
308
309
RTP処理部
MPEG4拡張ヘッダに必要な情報
暗号拡張ヘッダに必要な情報
301
315
302
304
306
MPEG4
データ
生成部
MPEG4
ペイロード
ヘッダ
付与部
データ
暗号部
暗号拡張
ヘッダ
付与部
RTP
基本ヘッダ
付与部
TCP/IP
及び
UDP/IP
処理部
リンク・
物理レイヤ
処理部
AV入力
MPEG4データ
MPEG4データ+ペイロードヘッダ
暗号化MPEG4データ
311
RTCP
送信部
307
認証・
鍵交換
処理部
フィードバック信号
RTCP
受信
解析部
310

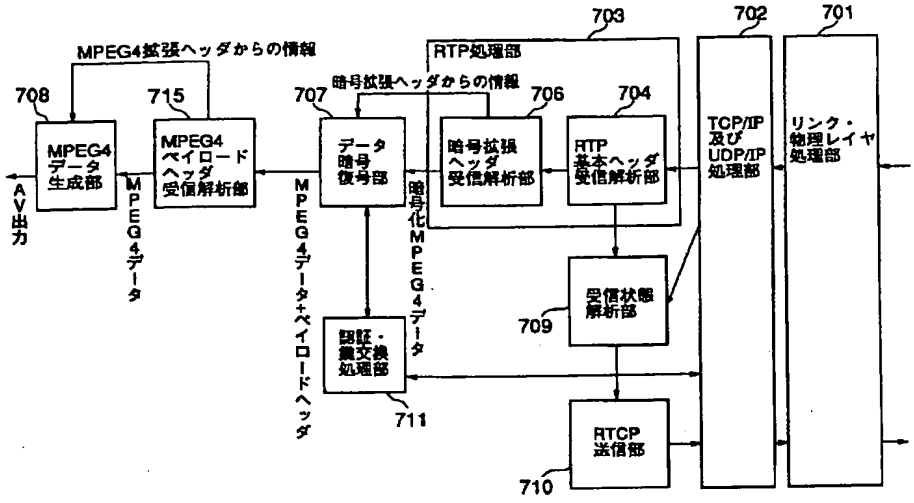
【図１８】


RTP基本ヘッダ
(Xビット=1；拡張ヘッダあり)
(ペイロードタイプ=暗号化データ)
暗号拡張ヘッダ
(ペイロードタイプ=MPEG4)

【図２１】


RTP基本ヘッダ
(Xビット=0；拡張ヘッダなし)
(ペイロードタイプ=暗号化データ)

【図１１】



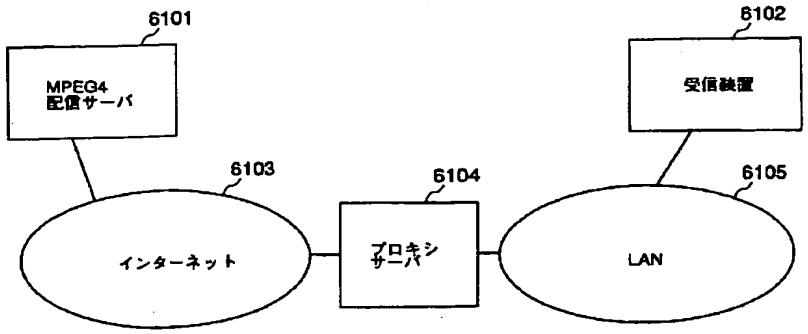
【図１３】

IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ（PT=MPEG4）
	暗号拡張ヘッダ （拡張ヘッダID=暗号拡張ヘッダ）
RTPペイロード	MPEG4ペイロードヘッダ
	[MPEG4データ]Kc （暗号化されたMEG4データ）

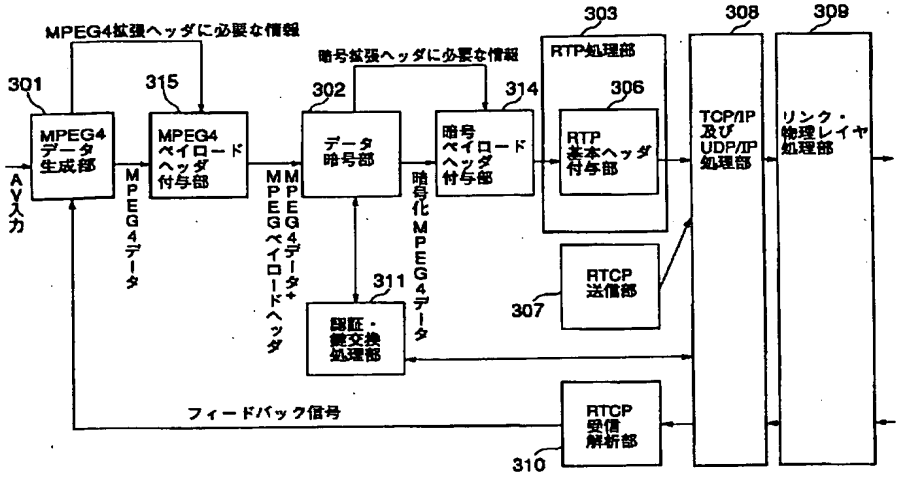
【図１６】

IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ（PT=暗号化MPEG4）
RTPペイロード	暗号拡張ヘッダ
	MPEG4ペイロードヘッダ
	[MPEG4データ]Kc （暗号化されたMEG4データ）

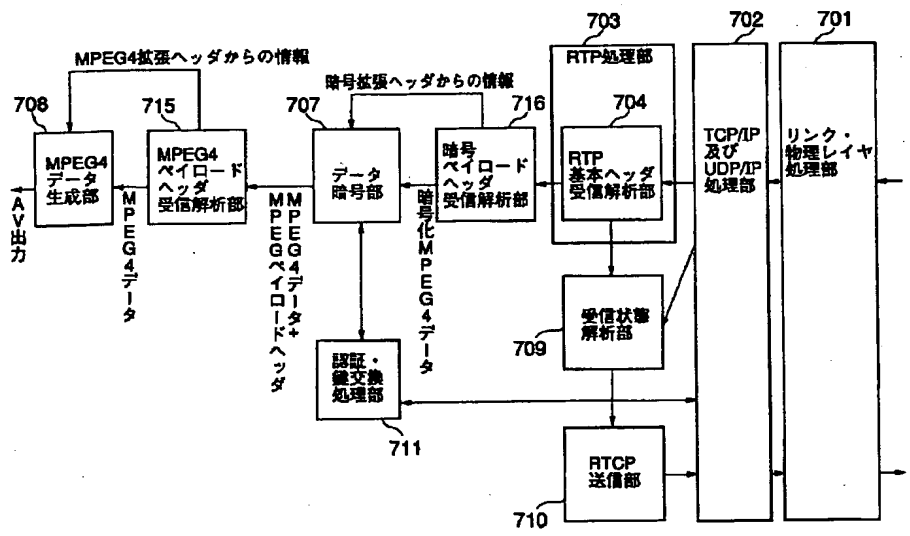
【図２３】



【図１４】



【図１７】



【図２７】

MIME基本ヘッダ MIME−Version:1.0 Message−ID:User1−1 Content−Type:Multipasrt/mixed boundary="−boundary1−"
暗号拡張ヘッダ Content−Type:application/x−encription 暗号方式表示フィールド（暗号方式＝M6） 暗号化有無フィールド（暗号あり） 暗号モードインジケータ(EMI)フィールド Even/Oddフィールド

【図１９】

	暗号化有無フィールド（暗号あり）
8ビット	ペイロードタイプフィールド（種別=MPEG4）
8ビット	暗号化有無フィールド（暗号あり）
8ビット	暗号方式表示フィールド（暗号方式=M6）
8ビット	暗号モードインジケータ（EMI）フィールド
8ビット	Even/Oddフィールド

【図２０】

IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ（PT=暗号化データ）
	暗号拡張ヘッダ（ペイロードタイプ=MPEG4）
RTPペイロード	MPEG4ペイロードヘッダ
	[MPEG4データ]Kc（暗号化されたMEG4データ）

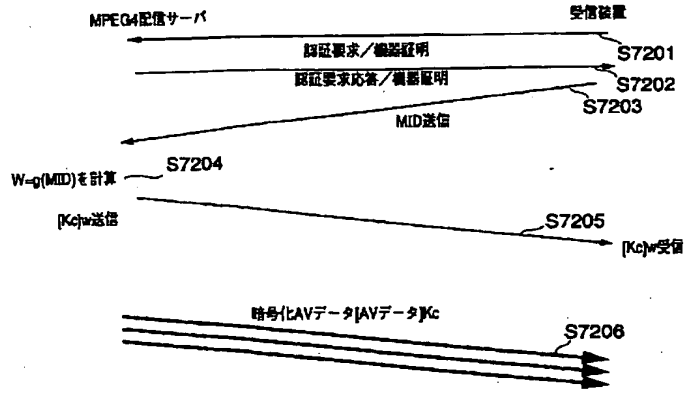
【図２２】

IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ（PT=暗号化データ）
RTPペイロード	暗号拡張ヘッダ（ペイロードタイプ=MPEG4）
	MPEG4ペイロードヘッダ
	[MPEG4データ]Kc（暗号化されたMEG4データ）

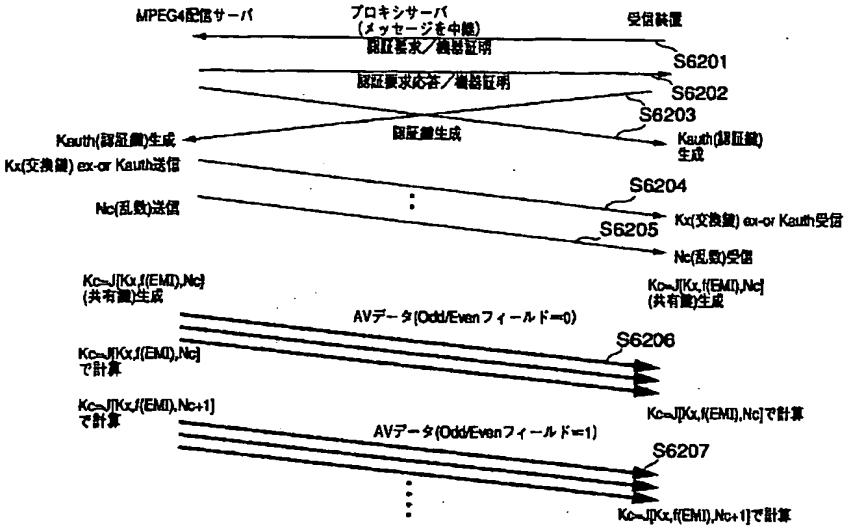
【図２６】

IPヘッダ(IPv4/IPv6)	
TCPヘッダ	
MIME基本ヘッダ	
Content−Type=application/X−encripsion	暗号拡張ヘッダ
Content−Type=application/X−MPEG4	MPEG4ペイロードヘッダ
	[MPEG4データ]Kc（暗号化されたMEG4データ）

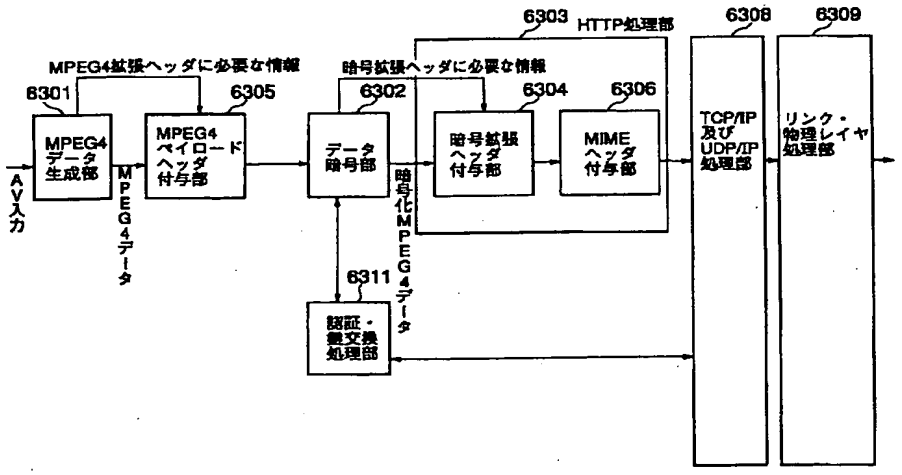
【図２９】



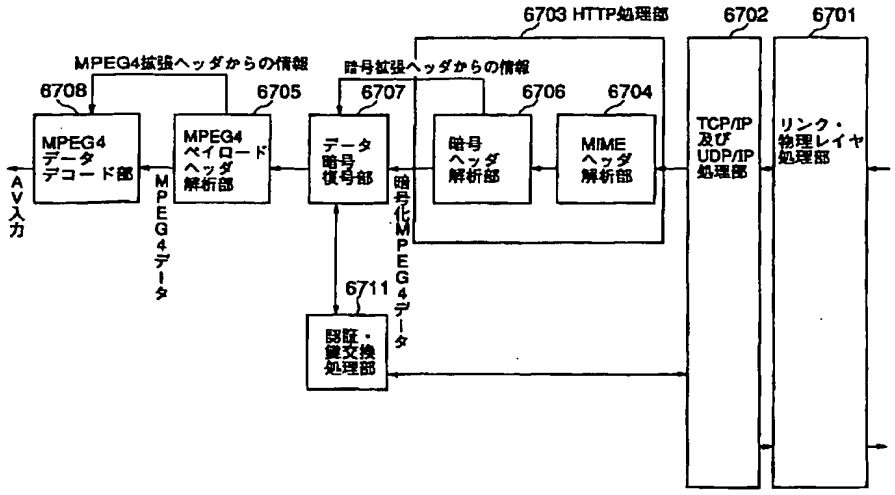
【図２４】



【図２５】



【図２８】



フロントページの続き

(72)発明者 友田 一郎
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 高畠 由彰
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 網 淳子
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内

Ｆターム(参考) 5C064 CA14 CB01 CC04
5J104 AA07 KA01 KA02 KA04 MA07 PA07
5K030 GA15 HA08 HB11 HB16 HB21 JA05 KA01 KA06 LA07 LD19 LD20
9A001 BB04 CC04 CZ06 DD10 EE01 EE04 EZ03 HZ27 JJ18 JZ19 JZ25 LL03